#2

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年 ８月２５日

出願番号
Application Number: 特願２０００－２５５８４０

出願人
Applicant(s): 株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ４月２７日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号 出証特２００１－３０３５９

【書類名】　特許願

【整理番号】　A000004877

【提出日】　平成12年 8月25日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 13/00

【発明の名称】　電子機器及び接続制御方法

【請求項の数】　19

【発明者】

【住所又は居所】　東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

【氏名】　伊藤　隆文

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子機器及び接続制御方法

【特許請求の範囲】

【請求項１】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する通信手段を備えた電子機器であって、

第１の状態と第２の状態を切り換え可能なスイッチと、

このスイッチが第１の状態に設定されている場合には、上記特定の識別コードによる認証を禁止する認証禁止手段と、

上記スイッチが第２の状態に設定されている場合には、上記特定の識別コードによる認証を許可する認証許可手段と

を具備したことを特徴とする電子機器。

【請求項２】　上記スイッチが第２の状態に設定されてから所定時間経過したか否かを検知する時間検知手段と、

この時間検知手段により上記スイッチが第２の状態に設定されてから所定時間経過したことが検知された場合には、上記特定の識別コードによる認証を禁止する制御手段と

を具備したことを特徴とする請求項１記載の電子機器。

【請求項３】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

他の機器との間で接続を行うための各種管理情報を記憶する管理情報記憶手段と、

第１の状態と第２の状態を切り換え可能なスイッチと、

このスイッチが第１の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更を禁止する変更禁止手段と、

上記スイッチが第２の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更を許可する変更許可手段と

を具備したことを特徴とする電子機器。

【請求項４】　上記スイッチが第２の状態に設定されてから所定時間経過したか否かを検知する時間検知手段と、

この時間検知手段により上記スイッチが第２の状態に設定されてから所定時間経過したことが検知された場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更を禁止する制御手段と、

を具備したことを特徴とする請求項３記載の電子機器。

【請求項５】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

リンクの張られた他の機器それぞれの機器コードを記憶する機器コード記憶手段と、

他の機器から接続要求があったときに、当該機器の機器コードが上記機器コード記憶手段に記憶されていない場合には、当該機器に対して上記特定の識別コードによる認証を行う認証手段と、

この認証手段によって認証エラーと判定された場合には、当該機器の機器コードとそのエラー回数とを対応付けて記憶する認証エラー記憶手段と、

この認証エラー記憶手段に記憶されたエラー回数が所定回数を越えた場合には対応する機器コードを有する機器からの接続要求を拒否する制御手段と

を具備したことを特徴とする電子機器。

【請求項６】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行う認証手段と、

この認証手段によって認証可と判定された機器とのリンク情報を作成するリンク情報作成手段と、

このリンク情報作成手段によって作成されたリンク情報を該当機器と対応付けて登録するリンク情報登録手段と、

このリンク情報登録手段によるリンク情報の登録機器数が許容件数を越えた場合に所定の規則に従って不要と判定される機器のリンク情報を削除する削除手段と

を具備したことを特徴とする電子機器。

【請求項７】　上記リンク情報登録手段は、各機器それぞれのリンク情報に

対応付けて、各機器それぞれの最終接続時刻を共に記憶し、

上記削除手段は、上記リンク情報登録手段に登録されたリンク情報のうち、その最終接続時刻の最も古い機器のリンク情報を削除することを特徴とする請求項６記載の電子機器。

【請求項８】　上記リンク情報記憶手段は、各機器それぞれのリンク情報に対応付けて、その登録時刻を共に記憶し、

上記削除手段は、上記リンク情報登録手段に登録されたリンク情報のうち、その登録時刻の最も古い機器のリンク情報を削除することを特徴とする請求項６記載の電子機器。

【請求項９】　上記リンク情報記憶手段は、各機器それぞれのリンク情報に対応付けて、各機器それぞれの接続回数を共に記憶し、

上記削除手段は、上記リンク情報登録手段に登録されたリンク情報のうち、その接続回数の最も少ない機器のリンク情報を削除することを特徴とする請求項６記載の電子機器。

【請求項１０】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器であって、

上記特定の識別コードを記憶する識別コード記憶手段と、

他の機器から接続要求があったときに当該機器に対して上記識別コード記憶手段に記憶された特定の識別コードによる認証を行う認証手段と、

この認証手段によって認証可と判定された機器とのリンク情報を作成するリンク情報作成手段と、

このリンク情報作成手段によって作成されたリンク情報を該当機器と対応付けて登録するリンク情報登録手段と、

上記識別コード記憶手段に記憶された特定の識別コードが変更された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報を削除する削除手段と

を具備したことを特徴とする電子機器。

【請求項１１】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する電子機器であって、

上記他の機器と接続するための交換可能な無線通信ユニットと、

この無線通信ユニットの固有の識別コードを記憶するユニットコード記憶手段と、

他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行う認証手段と、

この認証手段によって認証可と判定された機器とのリンク情報を上記ユニットコード記憶手段に記憶された無線通信ユニットの識別コードに基づき作成するリンク情報作成手段と、

このリンク情報作成手段によって作成されたリンク情報を該当機器と対応付けて登録するリンク情報登録手段と、

上記無線通信ユニットが交換された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報を削除する削除手段と

を具備したことを特徴とする電子機器。

【請求項１２】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する通信手段を備えた電子機器に用いられる接続制御方法であって、

上記電子機器の本体に第１の状態と第２の状態を切り換え可能なスイッチを設けておき、

このスイッチが第１の状態に設定されている場合には、上記特定の識別コードによる認証を禁止し、

上記スイッチが第２の状態に設定されている場合には、上記特定の識別コードによる認証を許可することを特徴とする接続制御方法。

【請求項１３】　上記スイッチが第２の状態に設定されてから所定時間経過したか否かを検知したか否かを判断し、

上記スイッチが第２の状態に設定されてから所定時間経過した場合には、上記特定の識別コードによる認証を禁止することを特徴とする請求項１２記載の接続制御方法。

【請求項１４】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、

他の機器との間で接続を行うための各種管理情報を記憶したメモリを備え、

上記電子機器の本体に第１の状態と第２の状態を切り換え可能なスイッチを設けておき、

第１の状態と第２の状態を切り換え可能なスイッチと、

このスイッチが第１の状態に設定されている場合には、上記メモリに記憶されている各種管理情報の変更を禁止し、

上記スイッチが第２の状態に設定されている場合には、上記メモリに記憶されている各種管理情報の変更を許可することを特徴とする接続制御方法。

【請求項１５】　上記スイッチが第２の状態に設定されてから所定時間経過したか否かを判断し、

上記スイッチが第２の状態に設定されてから所定時間経過した場合には、上記メモリに記憶されている各種管理情報の変更を禁止することを特徴とする請求項１４記載の接続制御方法。

【請求項１６】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、

リンクの張られた他の機器それぞれの機器コードを第１のメモリに記憶しておき、

他の機器から接続要求があったときに、当該機器の機器コードが上記第１のメモリに記憶されていない場合には、当該機器に対して上記特定の識別コードによる認証を行い、

この認証により認証エラーと判定された場合には、当該機器の機器コードとそのエラー回数とを対応付けて第２のメモリに記憶し、

この第２のメモリに記憶されたエラー回数が所定回数を越えた場合には対応する機器コードを有する機器からの接続要求を拒否することを特徴とする接続制御方法。

【請求項１７】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、

他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行い、

この認証によって認証可と判定された機器とのリンク情報を作成し、

このリンク情報を該当機器と対応付けてメモリに登録し、

このメモリによるリンク情報の登録機器数が許容件数を越えた場合に所定の規則に従って不要と判定される機器のリンク情報を削除することを特徴とする接続制御方法。

【請求項１８】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要する無線通信手段を備えた電子機器に用いられる接続制御方法であって、

上記特定の識別コードを第１のメモリに記憶しておき、

他の機器から接続要求があったときに当該機器に対して上記第１のメモリに記憶された特定の識別コードによる認証を行い、

この認証によって認証可と判定された機器とのリンク情報を作成し、

このリンク情報を該当機器と対応付けて第２のメモリに登録し、

上記第１のメモリに記憶された特定の識別コードが変更された場合には、上記第２のメモリに登録されたすべてのリンク情報を削除することを特徴とする接続制御方法。

【請求項１９】　他の機器との間でリンクを張る際に特定の識別コードによる認証を要し、上記他の機器と接続するための交換可能な無線通信ユニットを備えた電子機器の接続制御方法であって、

上記無線通信ユニットの固有の識別コードを第１のメモリに記憶しておき、

他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証を行い、

この認証によって認証可と判定された機器とのリンク情報を上記メモリに記憶された無線通信ユニットの識別コードに基づき作成し、

このリンク情報を該当機器と対応付けて第２のメモリに登録し、

上記無線通信ユニットが交換された場合には、上記第２のメモリに登録されたすべてのリンク情報を削除することを特徴とする接続制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、他の機器との間でデータ通信を行う無線通信機能を備えた電子機器及び接続制御方法に関する。

【０００２】

【従来の技術】

近年、ＩｒＤＡ、Ｂｌｕｅｔｏｏｔｈ、ＨｏｍｅＲＦ等のパーソナルエリアの無線通信システムが注目されている。特に、ＢｌｕｅｔｏｏｔｈやＨｏｍｅＲＦは、ＩｒＤＡのような赤外線通信方式と比較して、指向性がない、透過性が高いなどの長所を有しており、今後の発展、普及が大いに期待されている。なお、Ｂｌｕｅｔｏｏｔｈは、近距離の無線通信規格であり、２．４ＧＨｚ帯のＩＳＭ（Industrial Science Medical）バンドを用いて１０ｍ以内あるいは１００ｍ以内の無線通信を実現するものである。

【０００３】

Ｂｌｕｅｔｏｏｔｈ、ＨｏｍｅＲＦ等の無線通信システムは、同時に複数の機器との接続が可能である他に、ＩｒＤＡのような赤外線通信方式と比較して伝送距離が例えば１０～１００ｍと比較的長いということも大きな特徴の一つである。これは使い勝手の向上という利点もあるが、その反面、無線により外部から容易にアクセスできるため、無線通信システムのセキュリティ、秘話性の確保等に関しては十分に注意する必要がある。

【０００４】

一般的な無線通信システムのセキュリティ方式としては、特許第２８７２９９６号の公報に記載されている方式が知られている。これは、電子鍵と無線端末装置からなるセキュリティシステムにおいて、セキュリティを強化するために、同一鍵の連続使用を禁止し、紛失や盗難に対しての安全性を高めたものである。

【０００５】

また、Ｂｌｕｅｔｏｏｔｈでは、以下のようなユーザ認証によるセキュリティ方式が採用されている。

【０００６】

Ｂｌｕｅｔｏｏｔｈにおけるユーザ認証は、機器に設定するユニークな認証パスワードと、この認証パスワード及び機器固有のＩＤ（ＩＥＥＥが管理、発番する４８ビットのアドレス）等により作成される暗号鍵との２つにより管理されている。上記認証パスワードはＰＩＮ（Personal Identification Number）コードと呼ばれ、任意の文字列で構成される。上記暗号鍵はリンクキーと呼ばれ、ユーザ認証の他にデータの暗号化などにも用いられる。

【０００７】

今、機器Ａが機器Ｂに対してアクセスする場合を考える。

【０００８】

機器Ａと機器Ｂが初めて接続される状況においては、機器Ａは機器ＢのＰＩＮコードを入力する必要がある。機器Ａから入力されたＰＩＮコードが正しいと判定された場合には、機器Ｂは認証可としてリンクを開設して接続を許可する。このとき、機器Ｂは自身のＰＩＮコード及び機器ＡのＩＤに乱数を掛け合わせるなどして機器Ａのリンクキーを作成し、これを機器ＡのＩＤと共にリンクキーテーブルに保存しておく。なお、リンクキーを作成する場合に、各機器間で互いにリンクキーを交換する相手のＰＩＮコードや自身のＩＤも用いる。

【０００９】

一方、機器Ａが以前に機器Ｂに接続されたことがあれば、既に機器Ａのリンクキーが上記リンクテーブルに登録されているので、ＰＩＮコードの入力を省いて、上記リンクキーによる認証を行う。

【００１０】

【発明が解決しようとする課題】

Ｂｌｕｅｔｏｏｔｈを利用した機器として様々なものがあり、その１つとして、モデムアクセスポイントと呼ばれる回線接続機器がある。このモデムアクセスポイントは公衆回線への接続機能を備えたものであり、これにＢｌｕｅｔｏｏｔｈの通信機能を付加すれば、他のＢｌｕｅｔｏｏｔｈ対応機器との間で無線による接続が可能となる。したがって、外部機器からモデムアクセスポイントに無線によりアクセスすれば、外部機器側ではモジュラーケーブルの接続を必要とせず

に、公衆回線に接続してインターネット等の利用を受けることができる。この場合、モデムアクセスポイントへのアクセスには、上述したＰＩＮコードまたはリンクキーによる認証が行われており、認証可と判定された外部機器のみがモデムアクセスポイントへの接続が許される。

【００１１】

しかしながら、モデムアクセスポイントのＰＩＮコードが何らかの手段で本来の使用者以外の者に知られた場合、そのＰＩＮコードを使用してモデムアクセスポイントに不正アクセスする可能性がある。モデムアクセスポイントの場合には、公衆回線の接続によって回線使用料金が生じるため、不正アクセスは重大な問題となる。

【００１２】

また、通常、モデムアクセスポイントは目立たない場所に設置され、かつ、電源が常時ＯＮになっていることが多い。このため、管理者が知らないうちに、外部からモデムアクセスポイントに不正アクセスする可能性が高い。

【００１３】

本発明は上記のような点を解決するためになされたもので、他の機器からの不正アクセスを防止してセキュリティを確保することのできる電子機器及び接続制御方法を提供することを目的とする。

【００１４】

【課題を解決するための手段】

すなわち、本発明の請求項１に係る電子機器では、他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、第１の状態と第２の状態を切り換え可能なスイッチが第１の状態に設定されている場合には、上記特定の識別コードによる認証が禁止され、また、上記スイッチが第２の状態に設定されている場合には、上記特定の識別コードによる認証が許可されるので、他の機器のユーザは、上記特定の識別コードを知っていても、上記スイッチを第１の状態に設定操作しない限り、当該機器とのリンクを張ることができないことになる。

【００１５】

また、本発明の請求項２に係る電子機器では、前記請求項１に係る電子機器に

あって、上記スイッチが第２の状態に設定されてから所定時間経過したことが検知された場合には、上記特定の識別コードによる認証は禁止されるので、上記スイッチが第２の状態に設定されたままでも、所定時間経過の後は他の機器とのリンクを張ることができないようになる。

【００１６】

また、本発明の請求項３に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、他の機器との間で接続を行うための各種管理情報を記憶する管理情報記憶手段を有し、第１の状態と第２の状態を切り換え可能なスイッチが第１の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更が禁止され、また、上記スイッチが第２の状態に設定されている場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更が許可されるので、他の機器の不正ユーザがこの電子機器と接続できても、上記スイッチを第１の状態に設定操作しない限り、上記他の機器との接続のための各種管理情報の変更操作はできないことになる。

【００１７】

また、本発明の請求項４に係る電子機器では、前記請求項３に係る電子機器にあって、上記スイッチが第２の状態に設定されてから所定時間経過したことが検知された場合には、上記管理情報記憶手段に記憶されている各種管理情報の変更は禁止されるので、上記スイッチが第２の状態に設定されたままでも、所定時間経過の後は上記他の機器との接続のための各種管理情報の変更操作はできないないようになる。

【００１８】

また、本発明の請求項５に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、リンクの張られた他の機器それぞれの機器コードを記憶する機器コード記憶手段を有し、他の機器から接続要求があったときに、当該機器の機器コードが前記機器コード記憶手段に記憶されてない場合には、当該機器に対して上記特定の識別コードによる認証が行われ、認証エラーと判定された場合には、当該機器の機器コードとその

エラー回数とが対応付けられて認証エラー記憶手段に記憶される。そして、この認証エラー記憶手段に記憶されたエラー回数が所定回数を越えた場合には対応する機器コードを有する機器からの接続要求が拒否されるので、同一機器からの不正な接続の試みはできないようになる。

【００１９】

また、本発明の請求項６に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証が行われ、認証可と判定されると当該機器とのリンク情報が作成され、この作成されたリンク情報は該当機器と対応付けされてリンク情報登録手段に登録される。そして、このリンク情報登録手段によるリンク情報の登録機器数が許容件数を越えた場合には、その登録リンク情報のうち、例えば最終接続時刻の最も古い機器のリンク情報（請求項７）、又は登録時刻の最も古い機器のリンク情報（請求項８）、又は接続回数の最も少ない機器のリンク情報（請求項９）という不要なリンク情報が判定されて削除されるので、新たな接続機器とのリンク情報を接続可能性の低い機器のリンク情報と代えて登録できることになる。

【００２０】

また、本発明の請求項１０に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、上記特定の識別コードを記憶する識別コード記憶手段を有し、他の機器から接続要求があったときに当該機器に対して上記識別コード記憶手段に記憶された特定の識別コードによる認証が行われ、認証可と判定されると当該機器とのリンク情報が作成され、この作成されたリンク情報は該当機器と対応付けされてリンク情報登録手段に登録される。そして、上記識別コード記憶手段に記憶された特定の識別コードが変更された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報が削除されるので、上記特定の識別コードの書き換え後は当該新たな識別コードを知らないユーザによって他の機器との間でリンクが張られるのを防止できることになる。

【００２１】

また、本発明の請求項１１に係る電子機器では、無線通信により他の機器との間でリンクを張る際に特定の識別コードによる認証を要するもので、上記他の機器と接続するための交換可能な無線通信ユニットと、この無線通信ユニットの固有の識別コードを記憶するユニットコード記憶手段を有し、他の機器から接続要求があったときに当該機器に対して上記特定の識別コードによる認証が行われ、認証可と判定されると当該機器とのリンク情報が上記ユニットコード記憶手段に記憶された無線通信ユニットの識別コードに基づき作成され、この作成されたリンク情報は該当機器と対応付けされてリンク情報登録手段に登録される。そして、上記無線通信ユニットが交換された場合には、上記リンク情報登録手段に登録されたすべてのリンク情報が削除されるので、上記無線通信ユニットの交換後はそのユニット固有の識別コードに基づくリンク情報を作成し登録し直さないと、他の機器とのリンクが張れないことになる。

【００２２】

【発明の実施の形態】

以下、図面を参照して本発明の一実施形態を説明する。

【００２３】

図１は本発明の一実施形態に係る無線通信システムの外観構成を示す斜視図である。図１では、公衆回線の接続機能を備えた回線接続機器（以下、アクセスポイントと称す）１０と、このアクセスポイント１０との間で無線通信を行うパーソナルコンピュータ（以下、パソコンと称す）１００が示されている。

【００２４】

アクセスポイント１０およびパソコン１００には、無線通信カードとして、Ｂｌｕｅｔｏｏｔｈの無線通信規格に従ったＰＣカード（以下、ＢＴ－ＰＣカードと称す）２０が脱着自在に装着されている。アクセスポイント１０およびパソコン１００は、このＢＴ－ＰＣカード２０を装着することで、互いに無線によるデータ通信が可能となる。

【００２５】

パソコン１００は、ここではアクセスポイント１０にアクセスする外部機器として用いられる。このパソコン１００の本体１１４には、キーボード１１２や液

晶表示パネル１１６、カードスロット１１８が設けられている。

【００２６】

アクセスポイント１０は、モジュラケーブル１２を介して公衆回線１１に接続され、パソコン１００から無線送信されたデータを公衆回線１１に転送すると共に公衆回線１１から入力されたデータをパソコン１００に無線送信する。

【００２７】

図２乃至図６にアクセスポイント１０の構成を示す。

【００２８】

図２はアクセスポイント１０の分解斜視図、図３はアクセスポイント１０を縦置きで使用した状態を示す斜視図、図４はアクセスポイント１０の背面側を示す斜視図、図５はアクセスポイント１０を横置きで使用した状態を示す斜視図、アクセスポイント１０の底面側を示す斜視図である。

【００２９】

図２乃至図６に示すように、アクセスポイント１０は、例えば合成樹脂等によって形成されたほぼ矩形状の機器本体１４を備えている。この機器本体１４は、僅かに湾曲した前面１４ａ、この前面と対向したほぼ平坦な背面１４ｂ、対向する一対の側面１４ｃ、上面１４ｄ、および底面１４ｅを有している。そして、機器本体１４の底面１４ｅおよび背面１４ｂはそれぞれ第１および第２設置面を構成している。

【００３０】

アクセスポイント１０は、図３および図４に示すように、底面１４ｅを机面上等に載置することにより機器本体１４を縦置きとして使用し、あるいは、図５に示すように、背面１４ｂを机面上等に載置することにより機器本体１４を横置きとして使用することができる。また、背面１４ｂには、ピンやフック等を掛けるための２つの係合凹所１６が形成され、これらの係合凹所１６を利用することにより、機器本体１４をその背面が壁と対向した状態で壁掛け式としても使用することができる。

【００３１】

機器本体１４の一方の側面１４ｃには、押しボタン式の電源スイッチ１８が設

けられている。他方の側面１４ｃには、ＲＳ２３２Ｃコネクタ２２および電源接続用のＡＣアダプタ端子２３が設けられている。また、機器本体１４の前面１４ａには、アクセスポイント１０の動作状態を示す表示部として、複数のＬＥＤ２４が並んで設けられている。動作状態としては、例えば、電源オン（POWER ）、送信（SD）、受信（RD）、オフフック（OH）、後述するＢＴ－ＰＣカード２０のスタンバイ／アクティブ（STB/ACT ）状態等を表示する。

【００３２】

機器本体１４の上面１４ｄには、着脱自在な透明カバー１５と、後述するカードスロット２６のカード挿入口２８およびイジェクトボタン３０が設けられている。また、図６から分かるように、底面１４ｅには、アクセスポイント１０を公衆回線１１に接続するためのモジュラケーブル１２を接続可能な２つのモジュラジャック３２、左右一対のスライドスイッチ３４ａ、３４ｂ、１つのロータリスイッチ３５が設けられている。

【００３３】

底面１４ｅには、その周縁部に沿ってスカート部３６が立設され、その一部には切欠３７が形成されている。このスカート部３６は、機器本体１４を縦置きとして使用する際に脚部として機能する。上記モジュラジャック３２に接続されたモジュラケーブル１２は、切欠３７を通して外部に引き出される。従って、モジュラジャック３２にモジュラケーブル１２を接続した状態で機器本体１４を縦置きとして使用する場合でも、モジュラケーブル１２が邪魔になることなく、スカート部３６により機器本体１４を安定して支持することができる。

【００３４】

機器本体１４内には、保持部として機能するカードスロット２６が設けられ、このカードスロットのカード挿入口２８は機器本体の上面１４ｄに開口している。そして、このカードスロット２６には、カード挿入口２８を通して、ＢＴ－ＡＣカード２０を脱着自在に装着可能となっている。

【００３５】

次に、ＢＴ－ＰＣカード２０の構成について説明する。

【００３６】

図７はＢＴ－ＰＣカード２０の斜視図、図８はＢＴ－ＰＣカード２０の分解斜視図である。

【００３７】

図７および図８に示すように、ＢＴ－ＰＣカード２０は、ＰＣＭＣＩＡの規格に準拠したカード本体４０と、カード本体の一端側から突出している共にＢＴ規格に準拠した送受信部４２とを備えている。カード本体４０は、合成樹脂からなるほぼ矩形状の枠体４３を有する。この枠体４３は、カード本体４０内のカード基板４４の周縁部を支持している。カード基板４４の一端にはコネクタ４５が取り付けられ、また、カード基板の他端部はカード本体４０から突出している。

【００３８】

カード基板４４の一方の表面、ここでは上面４４ａ上には、複数の電子部品４６が実装されている。また、カード基板４４の他端部上面には、送受信部４２を構成するアンテナ部４６、送受信時に点灯するＬＥＤ４７およびヘッドフォン、マイクロフォン等を接続するためのヘッドセット部４８が設けられている。

【００３９】

そして、カード基板４４の上面および下面は、枠体４３に嵌合された一対の金属カバー５０ａ、５０ｂにより、他端部を除いて覆われている。

【００４０】

また、送受信部４２は合成樹脂からなるキャップ５１を有し、このキャップ５１はカード本体４０の他端に嵌合され、カード基板４４の他端部、およびこの他端部上面に実装されたアンテナ部４６、ＬＥＤ４７、ヘッドセット部４８を覆っている。

【００４１】

上記ＢＴ－ＰＣカード２０において、コネクタ４５が設けられている前端はカードスロット２６に対して挿入側端となる。そして、枠体４３の一方の側壁前端には、カード本体４０の上面、側面、前端面に開口した第１ガイド溝５２ａが形成され、また、枠体４３の他方の側壁前端には、カード本体４０の側面および前端面のみに開口した第２ガイド溝５２ｂが形成されている。これらの第１および第２ガイド溝５２ａ、５２ｂは、ＢＴ－ＰＣカード２０をカードスロット２６に

装着する際、ＢＴ－ＰＣカード２０の表裏の向きを規制する。

【００４２】

パソコン１００に装着されるＢＴ－ＰＣカード２０も同様の構成であり、図１に示すようにパソコン１００の側面部に設けられたカードスロット１１８を介して装着される。

【００４３】

このような構成のＢＴ－ＰＣカード２０をアクセスポイント１０、パソコン１００にそれぞれ装着することで、アクセスポイント１０とパソコン１００との間でＢｌｕｅｔｏｏｔｈの無線通信規格に従ったデータ通信が可能となる。

【００４４】

ところで、パソコン１００がアクセスポイント１０にアクセスする場合に、アクセスポイント１０とパソコン１００が初めて接続される状況においては、パソコン１００はアクセスポイント１０のＰＩＮコードを入力する必要がある。アクセスポイント１０は、パソコン１００から入力されたＰＩＮコードが正しければリンクを開設して接続を許可する。このとき、アクセスポイント１０はパソコン１００のＩＤや自身のＰＩＮコードなどを元にリンクキーを作成し、次回パソコン１００から接続要求があったときには、このリンクキーによる認証を行うことになる。

【００４５】

アクセスポイント１０のＰＩＮコード（認証パスワード）は予め接続が許可された使用者にのみ知らされているものである。しかし、何らかの手段（例えばコード解読専用のソフトウェアを使用するなどして）で本来の使用者以外の者に知られると、そのＰＩＮコードを用いてアクセスポイント１０に不正アクセスして、公衆回線１１を無断で使用する問題がある。

【００４６】

以下では、このような不正アクセスを防止することを主旨として説明する。

【００４７】

図９は本発明の無線通信システムの構成を示すブロック図であり、上記図１の構成と対応しており、アクセスポイント１０とパソコン１００とで無線通信シス

テムを構成してことが示されている。

【００４８】

ここで、本実施形態では、図１０に示すようにアクセスポイント１０の裏面など、目立たないの場所にスライドスイッチ３４ａ、３４ｂが設けられている。これらのスライドスイッチ３４ａ、３４ｂは２位置間を切り換え可能なスイッチであり、禁止モードと許可モードの切り換え操作を行うためのものであり。スライドスイッチ３４ａはＰＩＮコードによる認証動作（新規機器の登録動作）を禁止／許可し、スライドスイッチ３４ｂはセキュリティ情報のメンテナンス動作（ＰＩＮコードやリンクキーの変更動作）を禁止／許可する。

【００４９】

スライドスイッチ３４ａ、３４ｂの操作は基本的にはアクセスポイント１０の管理者が行い、通常はスライドスイッチ３４ａ、３４ｂ共に禁止状態に設定しておく。そして、アクセスポイント１０に新規機器の登録を行う場合に、管理者がスライドスイッチ３４ａを操作して許可状態に切り換える。

【００５０】

このように、本来の使用者が新たに接続を行う場合にスライドスイッチ３４ａを許可状態に切り換え、普段は禁止状態としておけば、本来の使用者以外の者がアクセスポイント１０のＰＩＮコードを入力して不正アクセスすることを防止することができる。

【００５１】

また、アクセスポイント１０のＰＩＮコードの変更や、各機器のリンクキーの削除といったモデムアクセスポイント１０内に記憶されたセキュリティ情報のメンテナンスは、外部（既に登録されている機器）からコマンドを入力することにより実行できる。このようなセキュリティ情報のメンテナンスをスライドスイッチ３４ｂが許可状態になっているときのみ実行可能とすることで、アクセスポイント１０内のセキュリティ情報を勝手にアクセスして変更してしまうことを防止する。

【００５２】

なお、スライドスイッチ３４ａ、３４ｂとは別に、図１１に示すようなロータ

リスイッチ３５を用いることでも良い。このロータリスイッチ３５は、少なくとも４つの位置間を切換え可能なものとし、第１の位置でＰＩＮコードによる認証動作（新規機器の登録動作）とセキュリティ情報のメンテナンス動作（ＰＩＮコードやリンクキーの変更動作）の両方を禁止し、第２の位置でＰＩＮコードによる認証動作のみを許可、第３の位置でセキュリティ情報のメンテナンス動作のみを許可、第４の位置でＰＩＮコードによる認証動作とセキュリティ情報のメンテナンス動作の両方を許可する。

【００５３】

図１２にスライドスイッチ３４ａ、３４ｂとロータリスイッチ３５との対応関係を示す。図中のＳＷ１はスライドスイッチ３４ａ、ＳＷ２はスライドスイッチ３４ｂを示し、ＯＦＦは禁止状態、ＯＮは許可状態を示している。また、１～４はロータリスイッチ３５の切換え位置を示している。

【００５４】

このようなスライドスイッチ３４ａ、３４ｂとロータリスイッチ３５との対応関係を表したテーブルをアクセスポイント１０に持たせておくことで、スライドスイッチ３４ａ、３４ｂまたはロータリスイッチ３５にてアクセスポイント１０の動作状態を切り換えることができる。ただし、ロータリスイッチ３５はスライドスイッチ３４ａ、３４ｂに比べて操作しずらいため、スライドスイッチ３４ａ、３４ｂを用いてアクセスポイント１０の動作状態を切り換えることの方が好ましい。以下では、スライドスイッチ３４ａ、３４ｂを用いてアクセスポイント１０の動作状態を切り換えるものとして説明する。

【００５５】

図１３はアクセスポイント１０とＢＴ－ＰＣカード２０の回路構成を示すブロック図である。

【００５６】

図１３に示すように、アクセスポイント１０は、アクセスポイント全体の動作を制御するＣＰＵ７２を備えている。このＣＰＵ７２にはＬＥＤ２４、スイッチ群３４ａ、３４ｂ、３５、ＰＣカードインターフェースとしてのコネクタ６０、ＲＯＭ７３、ＲＡＭ７４、不揮発性メモリ７５、ＲＴＣ（Ｒｅａｌ　Ｔｉｍｅ

Ｃｌｏｃｋ）回路７６などが接続される。また、ＡＣアダプタ端子２３から供給される電源は、電源供給部７７を介してＣＰＵ７２に供給される。

【００５７】

更に、アクセスポイント１０は、モジュラケーブル１２およびモジュラジャック３２を介して公衆回線１１に接続されるモデム部７０を備えている。このモデム部７０およびＲＳ２３２Ｃコネクタ２２は、切換えスイッチ７８を介してＣＰＵ７２に接続されている。なお、モデム部７０およびモジュラジャック３０は送受信部として機能する。

【００５８】

ＲＯＭ７３は、無線通信および公衆回線１１との通信プロトコル等を格納している。ＲＡＭ７４は、アクセスポイント１０の動作プログラム、デバイスドライバおよび無線通信プロトコルを含むドライバソフトを格納している。

【００５９】

また、このＲＡＭ７４には、ここではＰＩＮコードの認証動作を制御する第１の動作制御情報、セキュリティ情報のメンテナンス動作を制御する第２の動作制御情報、基準時刻情報ＴＭを格納しておくための各種格納部７４ａ～７４ｃなどが設けられている。

【００６０】

不揮発性メモリ７５としては、例えばＥＥＰＲＯＭが用いられる。この不揮発性メモリ７５には、後述するリンクテーブルＴ１および認証エラーテーブルＴ２が設けられていると共に、自身のＩＤ（ＢＴ－ＰＣカード２０に登録されている）を保持しておくためのＩＤ格納部７５ａや、自身のＰＩＮコード（ユーザが任意に作成した認証用パスワード）を保持しておくためのパスワード格納部７５ｂなどが設けられている。

【００６１】

ＲＴＣ回路７６は、現在の時刻を計時するための回路である。

【００６２】

モデム部７０は、ＢＴ－ＰＣカード２０から入力されたデジタルデータをアナログデータに変換し、モジュラジャック３２を介して公衆回線１１に転送し、ま

た、モジュラジャック３２を介して公衆回線１１から入力されたアナログデータをデジタルデータに変換し、ＣＰＵ７２に転送する。

【００６３】

ＲＣ２３２Ｃコネクタ２２は、図示せぬＲＳ２３２Ｃケーブルを介してパソコン１００等の外部機器とアクセスポイント１０とをシリアル接続するために設けられている。例えば、ＲＣ２３２Ｃコネクタ２２およびＲＳ２３２Ｃケーブルを介してアクセスポイント１０にＩＳＤＮターミナルアダプタに接続し、ＢＴ－ＰＣカード２０から入力されたデジタルデータをそのまま伝送することも可能である。

【００６４】

切換えスイッチ７８は、モデム部７０およびモジュラジャック３２による公衆回線１１との接続と、ＲＳ２３２Ｃコネクタ２２による他の電子機器との接続とを切り換える。

【００６５】

一方、このアクセスポイント１０に装着されるＢＴ－ＰＣカード２０は、ＢＴ規格の無線モジュールとして、アンテナ部４６、ＲＦ部８０、ベースバンド部８１、メモリ８２、水晶発振部８３、ヘッドセット部４８、ＡＤ／ＤＡ変換部８４、ＬＥＤ４７を備えている。

【００６６】

ＢＴ－ＰＣカード２０とアクセスポイント１０とのデータの送受信はコネクタ４５を介して行う。アンテナ部４６は、無線通信を実行するための電波の送信、受信を行い、使用する周波数帯域はＢＴ規格の２．４～２．５ＧＨｚとなっている。ＲＦ部８０は、使用する所定の無線電波の周波数で通信が実行可能な信号処理を行う。

【００６７】

また、ベースバンド部８１は、アンテナ部４６、ＲＦ部８０を介して入力されたデータをデジタル処理し、アクセスポイント１０で処理可能なデータに変換してメモリ８２に格納し、アクセスポイントとの間でデータの授受を行う。なお、ここではメモリ８２にＩＤが予め記憶されているものとする。実際には、図示せ

ぬ書き換え不可メモリに予めＢＴ－ＰＣカード２０に割り付けられたＩＤが記憶されており、ＢＴ－ＰＣカード２０装着時にこのＢＴ－ＰＣカード２０のＩＤが機器固有の識別情報として不揮発性メモリ７５に書き込まれる。

【００６８】

ＬＥＤ４７は、例えばデータの送受信時に点灯する。水晶発振部８３は、ＲＦ部８０で使用する基準波を供給する。ヘッドセット部４８は、ヘッドフォンとマイクロフォンとを有するヘッドセットを接続し、音声信号の入出力を行う。また、ＡＤ／ＤＡ変換部８４は、ヘッドセット部４８から入力されたアナログの音声信号をデジタルデータに変換すると共に、アクセスポイント１０からベースバンド部８１を介して入力されたデジタルの音声信号をアナログデータに変換してヘッドセット部４８に出力する。

【００６９】

図１４はである。アクセスポイント１０に外部機器として接続されるパソコン１００とＢＴ－ＰＣカード２０の回路構成を示すブロック図。

【００７０】

パソコン１００には、図１に示すようにキーボード１１２が設けられた本体１１４と、この本体１１４に開閉自在に設けられた液晶表示パネル１１６とを有している。本体１１４にはカードスロット１１８が設けられ、このカードスロット１１８にはＢＴ－ＰＣカード２０が脱着自在に装着されている。カードスロット１１８の構成は上述したアクセスポイント１０のカードスロット２６とほぼ同一である。また、ＢＴ－ＰＣカード２０はアクセスポイント１０と共通であり、その内部構成は図１３と同様であるため、ここではその説明を省略する。

【００７１】

また、パソコン１００には、ＢＴ－ＰＣカード２０との間でデータの送受信を行うＰＣＭＣＩＡ規格のインターフェースコネクタ１２０と、パソコン全体の動作を制御するＣＰＵ１２２を備えている。ＣＰＵ１２２には、ＵＳＢ１２４、ＲＯＭ１２６、ＲＡＭ１２８などが接続されている。

【００７２】

ＵＳＢ１２４は、例えばアクセスポイント１０とＲＳ２３２Ｃコネクタ２２を

介してシリアル接続する際に使用する。ＲＯＭ１２６には、プログラム等のデータが記憶されている。ＲＡＭ１２８には、ＣＰＵ１２２の処理動作に必要な各種のデータが記憶される。また、このＲＡＭ１２８には、パソコン１００に設定されたＰＩＮコード（ユーザが任意に作成した認証パスワード）や、ＢＴ－ＰＣカード２０から読み込んだＩＤを格納したおくための各種データ格納部が設けられている。

【００７３】

次に、アクセスポイント１０が管理しているリンクテーブルＴ１および認証エラーテーブルＴ２の構成について説明する。

【００７４】

図１５はリンクテーブルＴ１の構成を示す図である。

【００７５】

リンクテーブルＴ１には、各機器に固有のＩＤ（アドレス）、そのＩＤなどを元に作成されたリンクキー、最終接続時刻、データ有無フラグが登録される。

【００７６】

上述したように、アクセスポイント１０では、新たな機器（リンクテーブルＴ１に未登録の機器）から接続要求があったときにはＰＩＮコードによる認証を行い、認証ＯＫの場合にその機器のＩＤなどを元にリンクキーを作成し、そのリンクキーをＩＤと共にリンクテーブルＴ１に登録する。また、このときの接続時刻をＲＴＣ回路７６から取得してリンクテーブルＴ１に登録しておく。上記接続時刻は機器接続時にその都度更新される。なお、データ有無フラグは当該レコード欄にデータが登録されているか否かを示すものである。

【００７７】

図１６は認証エラーテーブルＴ２の構成を示す図である。

【００７８】

認証エラーテーブルＴ２は、各機器に固有のＩＤ（アドレス）、認証エラー回数、最終接続時刻、データ有無フラグが登録される。

【００７９】

アクセスポイント１０は、ＰＩＮコードによる認証の際に認証エラーと判定さ

れた機器に対し、その機器のＩＤと認証エラー回数とを対応付けて認証エラーテーブルＴ２に登録しておく。認証エラー回数の初期値は「１」であり、機器が認証エラーと判定される毎に更新される。また、このときの接続時刻をＲＴＣ回路７６から取得して認証エラーテーブルＴ２に登録しておく。上記接続時刻は機器接続時にその都度更新される。なお、データ有無フラグは当該レコード欄にデータが登録されているか否かを示すものである。

【００８０】

リンクテーブルＴ１及び認証エラーテーブルＴ２の登録数は不揮発性メモリ７５の容量に応じて決められており、図１５の例ではリンクテーブルＴ１の最大登録件数はＮ件、図１６の例では認証エラーテーブルＴ２の最大登録件数はＭ件である。

【００８１】

次に、本システムの動作について説明する。

【００８２】

ここでは、アクセスポイント１０に対する不正アクセスを防止するための処理として、（ａ）スイッチによる動作状態の切り換え処理、（ｂ）外部機器との接続処理、（ｃ）セキュリティ情報のメンテナンス処理、（ｄ）接続時の認証エラー処理に分けて説明する。

【００８３】

（ａ）スイッチによる動作状態の切り換え処理

上述したように、アクセスポイント１０の裏面には、アクセスポイント１０の動作状態を切換えるためのスライドスイッチ３４ａ、３４ｂが設けられている。スライドスイッチ３４ａはＰＩＮコードによる認証動作を禁止状態または許可状態とするものであり、スライドスイッチ３４ｂはセキュリティ情報のメンテナンス動作を禁止状態または許可状態とするものである。

【００８４】

ここで、スライドスイッチ３４ａによる動作状態の切換え処理について説明する。

【００８５】

図１７はアクセスポイント１０に設けられたスライドスイッチ３４ａによる動作状態の切換え処理を示すフローチャートである。なお、図１７はアクセスポイント１０のＣＰＵ７２が実行するプログラムの処理を示したものである。また、図中ＳＷ１はスライドスイッチ３４ａのことである。

【００８６】

アクセスポイント１０では、スライドスイッチ３４ａの状態を常に監視している。アクセスポイント１０は、スライドスイッチ３４ａが禁止状態から許可状態に切り換えられたことを検知すると（ステップＡ１１のＹｅｓ）、まず、図１３に示すＲＴＣ回路７６から現在時刻を取得し、この時刻を基準時刻情報ＴＭとしてＲＡＭ７４内の基準時刻格納部７４ｃにセットする（ステップＡ１２）。そして、ＰＩＮコードの認証動作を許可とする第１の動作制御情報をＲＡＭ７４内の第１の動作制御情報格納部７４ａにセットする（ステップＡ１３）。

【００８７】

一方、アクセスポイント１０は、スライドスイッチ３４ａが許可状態から禁止状態に切り換えられたことを検知すると（ステップＡ１４のＹｅｓ）、ＰＩＮコードの認証動作を禁止とする第１の動作制御情報をＲＡＭ７４内の第１の動作制御情報格納部７４ａにセットする（ステップＡ１５）。

【００８８】

また、スライドスイッチ３４ａが禁止状態から許可状態に切り換えられた後に、その切り換え時にセットされた基準時刻情報ＴＭと現在時刻との差が所定時間以上になると、つまり、スライドスイッチ３４ａが許可状態に切り換えられてから所定時間経過すると（ステップＡ１６のＹｅｓ）、アクセスポイント１０は、スライドスイッチ３４ａの状態に関係なく、ＰＩＮコードの認証動作を禁止とする第１の動作制御情報を第１の動作制御情報格納部７４ａにセットする（ステップＡ１７）。

【００８９】

スライドスイッチ３４ｂについても同様である。

【００９０】

すなわち、スライドスイッチ３４ｂが禁止状態から許可状態に切り換えられる

と、そのときの時刻が基準時刻情報ＴＭとしてＲＡＭ７４内の基準時刻格納部７４ｃにセットされると共に、セキュリティ情報のメンテナンス動作を許可とする第２の動作制御情報がＲＡＭ７４内の第２の動作制御情報格納部７４ｂにセットされる。一方、スライドスイッチ３４ｂが許可状態から禁止状態に切り換えられると、セキュリティ情報のメンテナンス動作を禁止とする第２の動作制御情報がＲＡＭ７４内の第２の動作制御情報格納部７４ｂにセットされる。

【００９１】

更に、スライドスイッチ３４ｂが禁止状態から許可状態に切り換えられた後、その切り換え時にセットされた基準時刻情報ＴＭ（スライドスイッチ３４ａを管理するものとは別のものとする）と現在時刻との差が所定時間以上になると、つまり、スライドスイッチ３４ｂが許可状態に切り換えられてから所定時間経過すると、スライドスイッチ３４ｂの状態に関係なく、セキュリティ情報のメンテナンス動作を禁止とする第２の動作制御情報がＲＡＭ７４内の第２の動作制御情報格納部７４ｂにセットされる。

【００９２】

なお、上記所定時間は例えば１０分程度が妥当であるが、その時間は予め決められていても良いし、アクセスポイント１０の管理者が任意に設定できるようにしても良い。

【００９３】

（ｂ）外部機器との接続処理

次に、外部機器との接続処理について説明する。

【００９４】

図１８はアクセスポイント１０における外部機器との接続処理の動作を示すフローチャートである。なお、図１８はアクセスポイント１０のＣＰＵ７２が実行するプログラムの処理を示したものである。

【００９５】

例えば外部機器であるパソコン１００からアクセスポイント１０に対して、無線通信により接続要求が送られてくると、アクセスポイント１０は、まず、ＲＡＭ７４内の第１の動作制御情報格納部７４ａに格納された第１の動作制御情報に

基づいて、ＰＩＮコードによる認証動作が許可されているか否かをチェックする（ステップＢ１１）。

【００９６】

上述したように、スライドスイッチ３４ａが許可状態に切り換えられており、かつ、スライドスイッチ３４ａが許可状態に切り換えられてから所定時間経過していない場合に、第１の動作制御情報は許可を示している。また、スライドスイッチ３４ａが禁止状態に切り換えられているか、あるいは、スライドスイッチ３４ａが許可状態に切り換えられてから所定時間経過している場合に、第１の動作制御情報は禁止を示している。

【００９７】

ＰＩＮコードによる認証動作が許可されていれば（ステップＢ１２のＹｅｓ）、アクセスポイント１０は接続要求先のパソコン１００が初めての接続か否かをパソコン１００に対するリンクキーの有無によってチェックする（ステップＢ１３）。すなわち、アクセスポイント１０が持つリンクテーブルＴ１には、これまでにアクセスポイント１０に接続された機器のＩＤとリンクキーとが登録されている。このリンクテーブルＴ１にパソコン１００に対するリンクキーがなければ、言い換えれば、リンクテーブルＴ１にパソコン１００のＩＤが登録されていなければ、パソコン１００は初めての接続と判定される。

【００９８】

ここで、アクセスポイント１０とパソコン１００とが初めて接続される状況においては（ステップＢ１３のＹｅｓ）、パソコン１００からアクセスポイント１０のＰＩＮコードを入力する必要がある。

【００９９】

パソコン１００からＰＩＮコードが入力されると、アクセスポイント１０はこのＰＩＮコードによる認証を行う（ステップＢ１４）。上記ＰＩＮコードが正しい場合つまり不揮発性メモリ７５内のパスワード格納部７５ｂに格納された自身のＰＩＮコードと一致した場合には認証可と判定する（ステップＢ１５のＹｅｓ）。

【０１００】

ここで、ＰＩＮコードによる認証動作について、図２２を参照して具体的に説明する。

【０１０１】

今、機器Ａが機器Ｂに接続を行う場合を想定する。本実施形態では、機器Ａはパソコン１００、機器Ｂはアクセスポイント１０に相当する。また、図中のパスワードとは、アクセスポイント１０のＰＩＮコードのことである。

【０１０２】

図２２に示すように、まず、機器Ａがコネクション要求（接続要求）を送信する（ステップＳ１）。機器Ｂは機器Ａからのコネクション要求を受信すると、この受信データを解析し、問題がない場合にはコネクション確立のメッセージを機器Ａに送信し（ステップＳ２）、しかる後に、機器Ａ－Ｂ間でコネクションが確立する（ステップＳ３）。なお、この場合のコネクションとは、通信の低位レイヤのコネクションを意味するもので、例えば「仮のネットワークアドレスが与えられた」という状況を意味するものとし、必ずしも上位アプリケーションのサービスを意味するものではない。

【０１０３】

上記コネクションが確立した後、パスワードによる認証手続きが行なわれる。すなわち、機器Ｂは、上記コネクションが確立すると、機器Ａに認証要求を出力し、パスワードの入力を促す（ステップＳ４）。これにより、機器Ａのユーザは機器Ｂのパスワードを入力し、それを送信する（ステップＳ５）。

【０１０４】

上記パスワードを受信した機器Ｂは、自機のパスワードと受信したパスワードとを照合する。照合結果が間違っていれば、パスワードが違う旨のメッセージを機器Ａに返すが、照合結果に問題がなければ認証を完了する（ステップＳ６）。

【０１０５】

図１８に戻って、上記のようなＰＩＮコードによる認証動作が行われた結果、認証可と判定された場合に（ステップＢ１５のＹｅｓ）、アクセスポイント１０はリンクを開設し（ステップＢ１６）、パソコン１００に対するリンクキーを作成する（ステップＢ１７）。詳しくは、パソコン１００のＩＤを取得し、そのＩ

Ｄと自身のＰＩＮコードなどをアクセスポイント１０側で発生する乱数を掛け合わせるなどして、解読困難なリンクキーを作成する。そして、アクセスポイント１０は上記作成されたリンクキーをパソコン１００のＩＤと共にリンクテーブルＴ１に登録する（ステップＢ１８）。その際、ＲＴＣ回路７６から現在の時刻を取得し、そのときの時刻を最終接続時刻としてリンクテーブルＴ１に登録すると共に、データ有無フラグを「有」にセットしておく。

【０１０６】

ここで、リンクテーブルＴ１に新たな機器のデータを登録する際に、リンクテーブルＴ１に空きがなければ（データ有無フラグがすべて有の状態）、最終接続時刻の最も古い機器のデータをリンクテーブルＴ１から削除して、そこに新たな機器のデータを登録するものとする。このように、接続される可能性の低い機器のリンクキーの代わりに新たに接続された機器のリンクキーを登録することで、不揮発性メモリ７５に設けられるリンクテーブルＴ１の登録件数（図１５の例ではＮ件）の中で新たな接続相手を優先してＰＩＮコードを効率的に管理でき、使い勝手を向上させることができる。

【０１０７】

なお、例えば各機器の本機器に対するアクセス回数をリンクテーブルＴ１に記憶させておき、アクセス回数の最も少ない機器のデータを削除することでも良い。

【０１０８】

また、各機器のリンクテーブルＴ１への登録時刻をリンクテーブルＴ１に記憶させておき、その登録時刻の最も古い機器のデータを削除することでも良い。

【０１０９】

ＰＩＮコードによる認証がＯＫとされると、アクセスポイント１０とパソコン１００との接続が確立され、互いに無線によるデータ通信が可能となる（ステップＢ１９）。また、ＰＩＮコードによる認証がＮＧであった場合には（ステップＢ１５のＮｏ）、アクセスポイント１０はそのときの接続要求先であるパソコン１００との接続を拒否する。

【０１１０】

一方、ＰＩＮコードによる認証動作が禁止されている場合（ステップＢ１２のＮｏ）あるいはパソコン１００が以前にアクセスポイント１０に接続されたことがある場合には（ステップＢ１３のＮｏ）、アクセスポイント１０はリンクキーによる認証を行う（ステップＢ２０）。この場合、接続要求先のパソコン１００が以前にアクセスポイント１０に接続されたことがあれば、パソコン１００に対するリンクキーがリンクテーブルＴ１に登録されているので、そのリンクキーを用いて認証を行うことができる。認証ＯＫであれば（ステップＢ２１のＹｅｓ）、アクセスポイント１０はパソコン１００との接続を確立する（ステップＢ１９）。また、ＰＩＮコードによる認証がＮＧであった場合には（ステップＢ２１のＮｏ）、アクセスポイント１０はそのときの接続要求先であるパソコン１００との接続を拒否する。

【０１１１】

このように、ＰＩＮコードによる認証動作が許可されている場合のみ、新たな機器がアクセスポイント１０へのアクセスを試みることができる。したがって、普段はスライドスイッチ３４ａの操作によりＰＩＮコードによる認証動作を禁止しておけば、本来の使用者以外の者がアクセスポイント１０のＰＩＮコードを何らかの手段で入手したとしても、アクセスポイント１０に対してアクセスすることはできないため、公衆回線１１が無断で使用するなどの不正行為を防ぐことができる。

【０１１２】

また、アクセスポイント１０の管理者がスライドスイッチ３４ａを禁止状態に切り換えておくのを忘れたとしても、所定時間経過すると、スライドスイッチ３４ａの状態に関係なく、ＰＩＮコードによる認証動作が自動的に禁止されるため、アクセスポイント１０のセキュリティを強化することができる。

【０１１３】

（ｃ）セキュリティ情報のメンテナンス処理

次に、セキュリティ情報のメンテナンス処理について説明する。

【０１１４】

図１９はアクセスポイント１０におけるセキュリティ情報のメンテナンス処理

の動作を示すフローチャートである。なお、図１９はアクセスポイント１０のＣＰＵ７２が実行するプログラムの処理を示したものである。

【０１１５】

今、外部機器であるパソコン１００との接続が確立された状態で（ステップＣ１１）、パソコン１００からセキュリティ情報のメンテナンスコマンドが無線より送信されたものとする。セキュリティ情報のメンテナンスコマンドには、ＰＩＮコードの読み出しや書き換え、リンクテーブルＴ１の読み出しや削除などがある。

【０１１６】

アクセスポイント１０は上記メンテナンスコマンドを受信すると、まず、ＲＡＭ７４内の第２の動作制御情報格納部７４ｂに格納された第２の動作制御情報に基づいて、セキュリティ情報のメンテナンス動作が許可されているか否かをチェックする（ステップＣ１２）。

【０１１７】

上述したように、スライドスイッチ３４ｂが許可状態に切り換えられており、かつ、スライドスイッチ３４ｂが許可状態に切り換えられてから所定時間経過していない場合に、第２の動作制御情報は許可を示している。また、スライドスイッチ３４ｂが禁止状態に切り換えられているか、あるいは、スライドスイッチ３４ｂが許可状態に切り換えられてから所定時間経過している場合に、第２動作制御情報は禁止を示している。

【０１１８】

セキュリティ情報のメンテナンス動作が禁止されていれば（ステップＣ１３のＮｏ）、アクセスポイント１０は上記メンテナンスコマンドを拒否する（ステップＣ１４）。これにより、どのような外部機器であっても、セキュリティ情報のメンテナンスを行うことはできない。

【０１１９】

一方、セキュリティ情報のメンテナンス動作が許可されていれば（ステップＣ１３のＹｅｓ）、アクセスポイント１０は上記メンテナンスコマンドを実行する（ステップＣ１５）。その際、ＰＩＮコードの書き換えが行われた場合には（ス

テップＣ１６のＹｅｓ）、アクセスポイント１０はリンクテーブルＴ１のデータをすべて削除する（ステップＣ１７）。

【０１２０】

このように、セキュリティ情報のメンテナンス動作が許可されている場合のみ、外部機器からコマンドを送って、ＰＩＮコードの書き換え等を行うことができる。したがって、普段はスライドスイッチ３４ｂの操作によりセキュリティ情報のメンテナンス動作を禁止しておけば、勝手にセキュリティ情報をアクセスすることはできないため、アクセスポイント１０のセキュリティを確保できる。

【０１２１】

また、アクセスポイント１０の管理者がスライドスイッチ３４ｂを禁止状態に切り換えておくのを忘れたとしても、所定時間経過すると、スライドスイッチ３４ｂの状態に関係なく、セキュリティ情報のメンテナンス動作が自動的に禁止されるため、アクセスポイント１０のセキュリティを確保することができる。

【０１２２】

さらに、ＰＩＮコードが変更された場合には不正アクセス者によるデータの改竄の可能性を考慮してリンクテーブルＴ１のデータをすべてクリアしておくことで、セキュリティをさらに強化することができる。リンクテーブルＴ１をクリアした場合には、すべての外部機器に対して再度ＰＩＮコードの入力を求めることになる。この場合、アクセスポイント１０で新たに設定されたＰＩＮコードを知らないユーザはアクセスポイント１０へ接続することはできないことになる。

【０１２３】

（ｄ）接続時の認証エラー処理

次に、接続時の認証エラー処理について説明する。

【０１２４】

図２０および図２１はアクセスポイント１０における接続時の認証エラー処理の動作を示すフローチャートである。なお、図２０および図２１はアクセスポイント１０のＣＰＵ７２が実行するプログラムの処理を示したものである。

【０１２５】

今、外部機器であるパソコン１００のＩＤがリンクテーブルＴ１に登録されて

いないものとする。このパソコン１００から接続要求があると（ステップＤ１１）、アクセスポイント１０は認証エラーテーブルＴ２を参照する（ステップＤ１２）。認証エラーテーブルＴ２には、図１６に示すように、以前に認証エラーとなった機器のＩＤ等が登録されている。

【０１２６】

この認証エラーテーブルＴ２にパソコン１００のＩＤが登録されていなかった場合には（ステップＤ１３のＮｏ）、アクセスポイント１０は通常通りＰＩＮコードによる認証を行う（ステップＤ１４）。そして、認証ＯＫであれば、つまり、パソコン１００が入力したＰＩＮコードがアクセスポイント１０のＰＩＮコードと一致すれば（ステップＤ１５のＹｅｓ）、アクセスポイント１０はパソコン１００の接続を許可する（ステップＤ１６）。

【０１２７】

一方、認証エラーであった場合、つまり、パソコン１００が入力したＰＩＮコードがアクセスポイント１０のＰＩＮコードと一致しなかった場合には（ステップＤ１５のＮｏ）、アクセスポイント１０はパソコン１００の接続を拒否する（ステップＤ１７）。その際、アクセスポイント１０はパソコン１００のＩＤを取得し、そのＩＤを認証エラーテーブルＴ２に登録すると共に、上記ＩＤに対応したエラー回数を初期値“１”とし、さらに、ＲＴＣ回路７６から現在の時刻を取得して、その時刻を最終接続時刻として登録する（ステップＤ１８）。

【０１２８】

また、上記ステップＤ１３において、リンクテーブルＴ１に接続要求先のパソコン１００のＩＤが登録されていたとする。つまり、以前にパソコン１００から入力されたＰＩＮコードが正しくないとして拒否されていたとする。

【０１２９】

このような場合において、アクセスポイント１０は、まず、認証エラーテーブルＴ２内のパソコン１００のＩＤに対応したエラー回数が所定回数を越えているか否かをチェックする（ステップＤ１９）。その結果、エラー回数が所定回数以内であれば（ステップＤ１９のＮｏ）、アクセスポイント１０は通常通りＰＩＮコードによる認証を行う（ステップＤ２０）。そして、認証ＯＫであれば、つま

り、パソコン１００が入力したＰＩＮコードがアクセスポイント１０のＰＩＮコードと一致すれば（ステップＤ２１のＹｅｓ）、アクセスポイント１０はパソコン１００の接続を許可する（ステップＤ２２）。このとき、認証エラーテーブルＴ２からパソコン１００に関するデータを削除しておく（ステップＤ２３）。

【０１３０】

一方、エラー回数が所定回数を越えている場合には（ステップＤ１９のＮｏ）、パソコン１００は不正アクセス者であると判断し、パソコン１００の接続を拒否する（ステップＤ２４）。その際、認証エラーテーブルＴ２内の当該パソコン１００のエラー回数を更新すると共に、ＲＴＣ回路７６から現在の時刻を取得して最終接続時刻として更新する（ステップＤ２５）。また、上記ステップＤ２１において認証エラーとなった場合にも同様にであり、接続の拒否と共に認証エラーテーブルＴ２内の当該パソコン１００に関するデータの更新を行う（ステップＤ２４、Ｄ２５）。

【０１３１】

このように、ＰＩＮコードによる認証時に認証エラーとなった場合の回数をカウントしておき、同一機器の認証エラー回数が所定回数を超えた場合には当該機器の接続を完全に拒否することで、同じ機器が何度もＰＩＮコードを入力してアクセスポイント１０に不正にアクセスすることを防止して、アクセスポイント１０のセキュリティを強化することができる。

【０１３２】

なお、上記所定回数は例えば５回程度が妥当であるが、その回数は予め決められていても良いし、アクセスポイント１０の管理者が任意に設定できるようにしても良い。

【０１３３】

また、認証エラーテーブルＴ２に新たな機器のデータを登録する際に、認証エラーテーブルＴ２に空きがなければ（データ有無フラグがすべて有の状態）、最終接続時刻の最も古い機器のデータを認証エラーテーブルＴ２から削除して、そこに新たな機器のデータを登録する。このように、古いデータを削除することで、不揮発性メモリ７５に設けられる認証エラーテーブルＴ２の登録件数（図１６

の例ではM件）の中で新たな接続相手を優先して認証エラー回数を効率的に管理でき、使い勝手を向上させることができる。

【０１３４】

以上のように、アクセスポイント１０に設けられたスイッチの操作によりＰＩＮコードによる認証動作やセキュリティ情報のメンテナンス動作を禁止することで、外部からの不正なアクセスを防止してセキュリティを強化することができる。さらに、スイッチの状態に関係なく、所定時間経過後にはＰＩＮコードによる認証動作やセキュリティ情報のメンテナンス動作を自動的に禁止状態に切り換えることで、管理者がスイッチ操作を忘れたとしてもセキュリティを確保することができる。

【０１３５】

また、同じ機器から不正なＰＩＮコードの入力が何度もあった場合に、以後、その機器の接続を完全に拒否することで、正しいＰＩＮコードを知らない者が不正アクセスを試みることを防止することができる。

【０１３６】

また、不揮発性メモリ７５に設けられるリンクテーブルＴ１へのリンクキーの登録件数数が記憶可能な最大数に達した後、新たな接続相手とリンクキーを登録する場合には、一定の規則（接続時刻が古いものやアクセス頻度が低いものなど）に従って既に記憶されたリンクキーを削除してその領域に新たなリンクキーを登録することで、新たな接続相手を優先して、その以後の接続時におけるＰＩＮコード入力を不要にでき、使い勝手を向上させることができる。

【０１３７】

また、アクセスポイント１０内のＰＩＮコードが変更された場合に、リンクテーブルＴ１に登録されている各機器のリンクキーのすべてを削除して、接続時に新たなＰＩＮコードの入力を要求するようにしたことで、セキュリティを強化することができる。

【０１３８】

ところで、各機器に装着されるＢＴ－ＰＣカード２０にはＢＴモジュールのＩＤが登録されており、アクセスポイント１０にＢＴ－ＰＣカード２０が装着され

た場合、図１５に示すＣＰＵ７２はＢＴ－ＰＣカード２０に登録されているＩＤを機器固有の情報として、アクセスポイント１０内の不揮発性メモリ７５のＩＤ格納部７５ａに格納する。

【０１３９】

ここで、ＣＰＵ７２がＰＣカードインターフェースとしてのコネクタ６０を介してＢＴ－ＰＣカード２０が交換されたことを検知した場合、リンクテーブルＴ１のデータをすべて削除して、各機器が接続されたときに新たにリンクキーを作成し直すといった処理を行う。

【０１４０】

これは、ＢＴモジュール（ＩＤを記憶している）がＰＣカードなどの交換可能なユニットで構成されていた場合に、ユーザの手違いで最初にアクセスポイント１０に装着されていたＢＴモジュールとは別のＢＴモジュールが装着される可能性があるためである。つまり、リンクキーはＩＤなどを元に作成されるものであるため、ＢＴモジュール交換前のＩＤで作成されたリンクキーをそのまま残しておくと、ＢＴモジュール交換後のＩＤによって作成されるリンクキーとの矛盾が生じ、外部機器との接続ができなくなる。このような不具合を解消するため、ＢＴモジュールが交換された場合には、現在リンクテーブルＴ１に登録されているデータをすべて削除して、各機器が接続されたときに新たにリンクキーを作成し直すといった処理を行う。

【０１４１】

なお、本発明は、アクセスポイント１０から離れた場所にある外部機器から無線により不正アクセスする場合に特に有効であるが、アクセスポイント１０へのアクセス手段として必ずしも無線である必要はない。すなわち、例えば図１に示すアクセスポイント１０とパソコン１００とが通信ケーブルを介して接続されるようなシステムであっても、上記実施形態で同様の手法を適用することで不正アクセスを防止することができる。

【０１４２】

また、上記実施形態では、公衆回線１１の接続機能を備えたアクセスポイント１０を例にして説明したが、無線等により他機器との接続を行うための通信機能

を備えた機器であれば、そのすべての機器に本発明の手法を適用できるものである。

【０１４３】

また、各機器に用いられる無線通信モジュールとしては、ＰＣカード等の交換可能なユニットで構成されている必要はなく、機器内に内蔵されているものであっても良い。

【０１４４】

また、無線通信方式としては、Ｂｌｕｅｔｏｏｔｈに限らず、他の方式であっても良い。

【０１４５】

要するに、本発明は上記実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。更に、上記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば、実施形態で示される全構成要件から幾つかの構成要件が削除されても、「発明が解決しようとする課題」で述べた効果が解決でき、「発明の効果」の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【０１４６】

また、上述した実施形態において記載した手法は、コンピュータに実行させることのできるプログラムとして、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリなどの記録媒体に書き込んで各種装置に適用したり、通信媒体により伝送して各種装置に適用することも可能である。本装置を実現するコンピュータは、記録媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されることにより、上述した処理を実行する。

【０１４７】

【発明の効果】

以上詳記したように本発明によれば、スイッチの状態に応じて、特定の識別コードによる認証が禁止または許可される。したがって、上記特定の識別コードを

不正に知り得たとしても、上記スイッチを直接に設定操作しない限り、本機器とのリンクを張ることができない。さらに、所定時間経過後は上記特定の識別コードによる認証が自動的に禁止されるため、管理者がスイッチを禁止状態に戻し忘れたとしてもセキュリティを確保できる。

【０１４８】

また、他の機器との間で接続を行うための各種管理情報に対する変更操作がスイッチの状態によって禁止または許可される。したがって、他の機器の不正ユーザが本機器と接続できたとしても、上記スイッチを直接に設定操作しない限り、各種管理情報を勝手に変更することはできない。さらに、所定時間経過後は上記各種管理情報の変更が自動的に禁止されるため、管理者がスイッチを禁止状態に戻し忘れたとしてもセキュリティを確保できる。

【０１４９】

また、所定回数を越えて認証エラーとなった機器からの接続要求が拒否されるため、同一機器からの不正な接続の試みを防止できる。

【０１５０】

また、メモリの登録件数が一杯にある状態では、その中で接続の可能性の低いリンク情報が削除されて新たな機器のリンク情報が登録されるため、使い勝手を向上させることができる。

【０１５１】

また、特定の識別コードが変更された場合にメモリ内のすべてのリンク情報が削除されるので、新たな識別コードを知らないユーザからの不正アクセスを防止できる。

【０１５２】

また、交換可能な無線通信ユニットを備えた電子機器において、無線通信ユニットの交換があった場合に、メモリ内のすべてのリンク情報が削除されるので、交換前の無線通信ユニットの識別コードにより作成されたリンク情報と交換後の無線通信ユニットの識別コードにより作成されたリンク情報との矛盾をなくして、他の機器との接続ができなくなることを防止できる。

【図面の簡単な説明】

【図１】

本発明の一実施形態に係る無線通信システムの外観構成を示す斜視図。

【図２】

上記無線通信システムに用いられるアクセスポイントの分解斜視図。

【図３】

上記アクセスポイントを縦置きで使用した状態を示す斜視図。

【図４】

上記アクセスポイントの背面側を示す斜視図。

【図５】

上記アクセスポイントを横置きで使用した状態を示す斜視図。

【図６】

上記アクセスポイントの底面側を示す斜視図。

【図７】

上記アクセスポイントに装着されるＢＴ－ＰＣカードの斜視図。

【図８】

上記ＢＴ－ＰＣカードの分解斜視図。

【図９】

上記無線通信システムの構成を示すブロック図。

【図１０】

上記アクセスポイントに設けられたスライドスイッチの構成を示す図。

【図１１】

上記アクセスポイントに設けられたロータリスイッチの構成を示す図。

【図１２】

上記スライドスイッチと上記ロータリスイッチとの対応関係を示す図。

【図１３】

上記アクセスポイントとＢＴ－ＰＣカードの回路構成を示すブロック図。

【図１４】

上記アクセスポイントに外部機器として接続されるパソコンとＢＴ－ＰＣカードの回路構成を示すブロック図。

【図１５】

上記アクセスポイントに設けられたリンクテーブルの構成を示す図。

【図１６】

上記アクセスポイントに設けられた認証エラーテーブルの構成を示す図。

【図１７】

上記アクセスポイントに設けられたスライドスイッチによる動作状態の切換え処理を示すフローチャート。

【図１８】

上記アクセスポイントにおける外部機器との接続処理の動作を示すフローチャート。

【図１９】

上記アクセスポイントにおけるセキュリティ情報のメンテナンス処理の動作を示すフローチャート。

【図２０】

上記アクセスポイントにおける接続時の認証エラー処理の動作を示すフローチャート。

【図２１】

上記アクセスポイントにおける接続時の認証エラー処理の動作を示すフローチャート。

【図２２】

ＰＩＮコードによる認証動作を説明するための図。

【符号の説明】

１０…アクセスポイント

１２…モジュラケーブル

１４…機器本体

２０…ＢＴ－ＰＣカード

３４ａ、３４ｂ…スライドスイッチ

３５…ロータリスイッチ

４０…カード本体

４２…送受信部

４６…アンテナ部

４５、６０…コネクタ

７０…モデム部

７２…ＣＰＵ

７４…ＲＡＭ

７４ａ…第１の動作制御情報格納部

７４ｂ…第２の動作制御情報格納部

７４ｃ…基準時刻格納部

７５…不揮発性メモリ

７５ａ…ＩＤ格納部

７５ｂ…パスワード格納部

Ｔ１…リンクテーブル

Ｔ２…認証エラーテーブル

７６…ＲＴＣ回路

１００…パソコン

１１２…キーボード

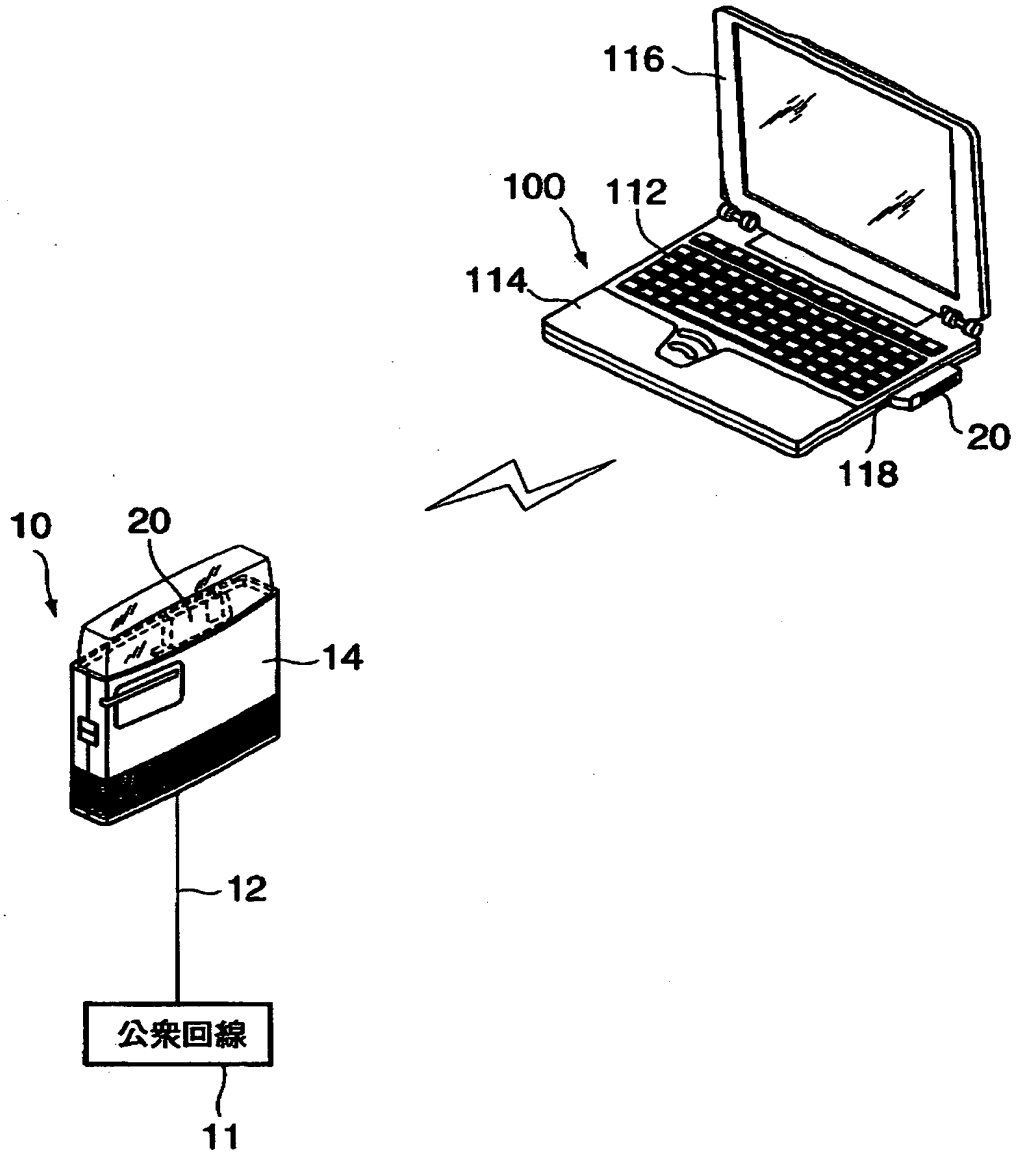
１１６…ＬＣＤパネル

１２０…インターフェースコネクタ

１２２…ＣＰＵ

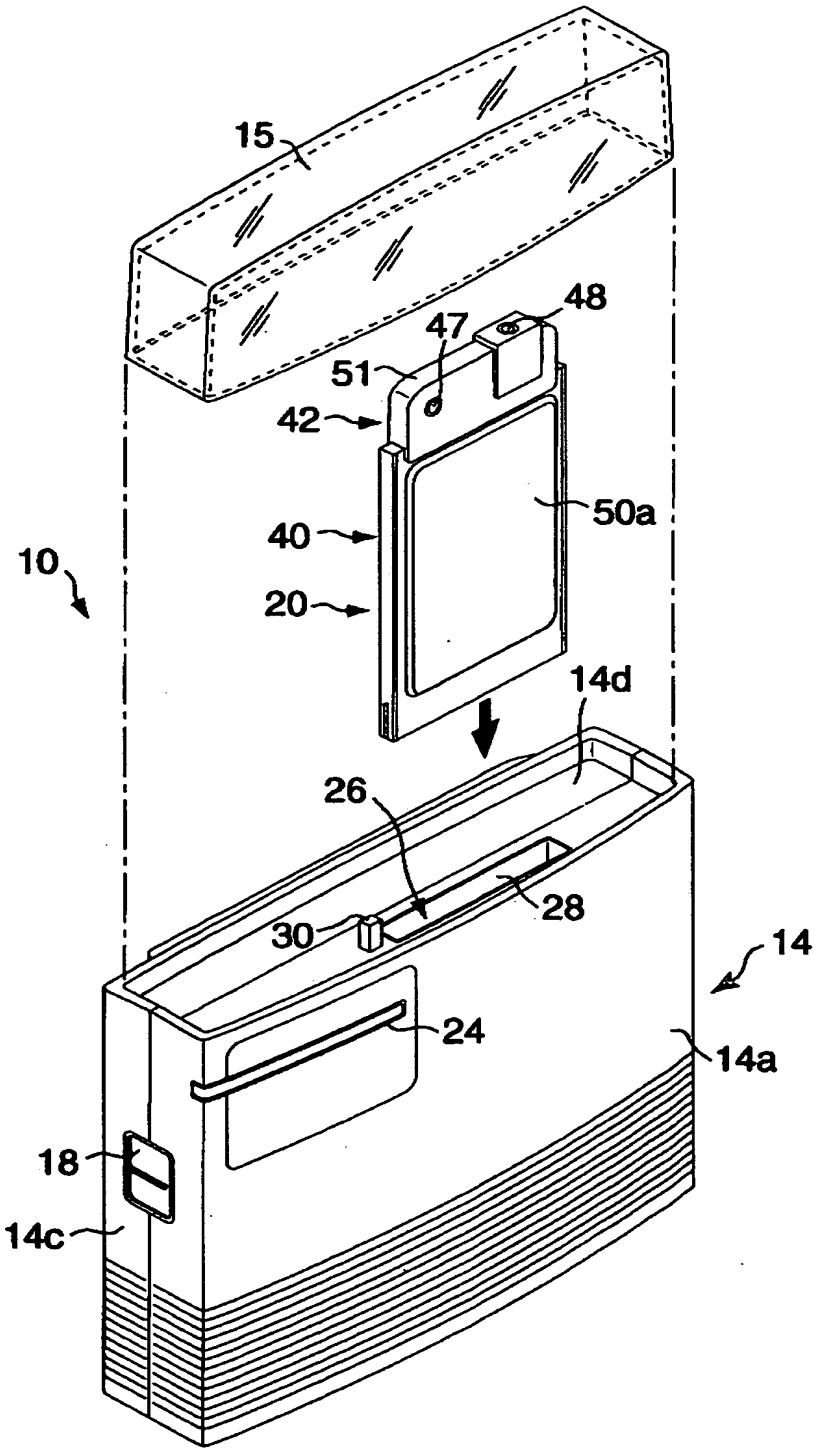
【書類名】　　図面

【図１】

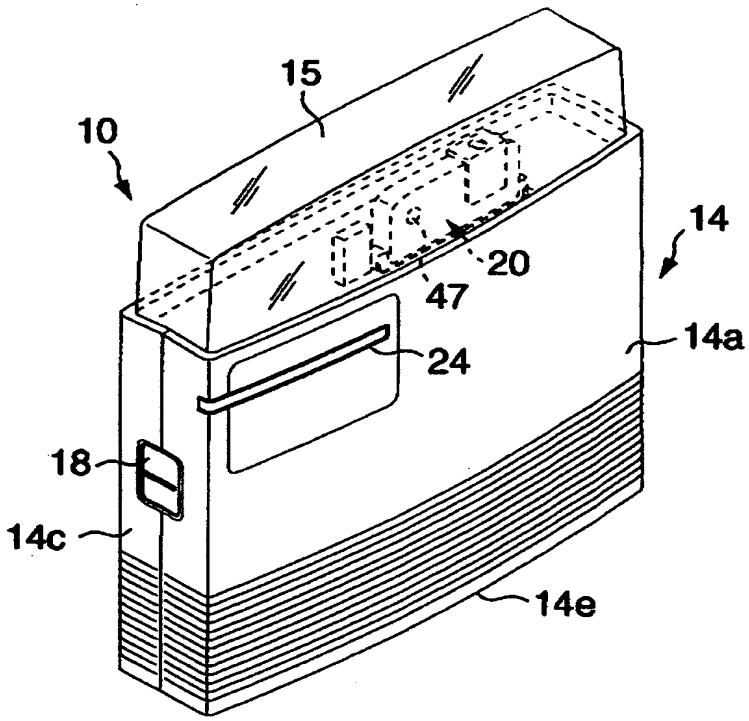


出証特２００１－３０３５９７７

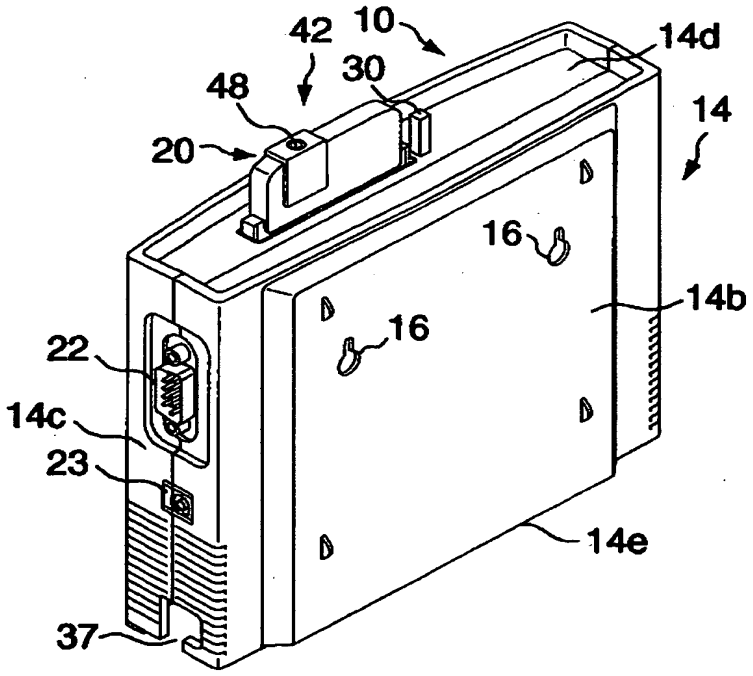
【図２】



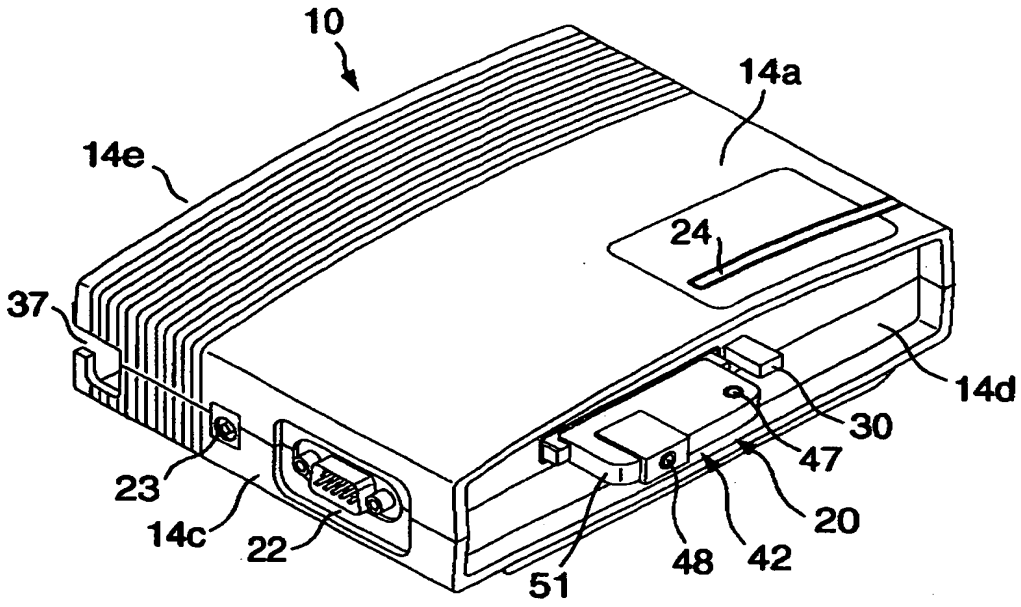
【図３】


15
10
14
20
47
14a
24
18
14c
14e

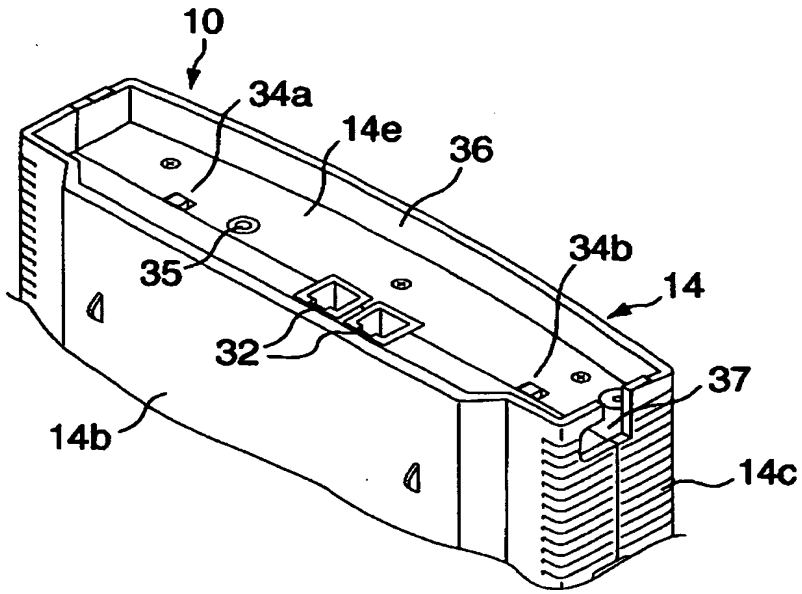
【図４】


42
10
14d
30
48
14
20
16
14b
16
22
14c
23
14e
37

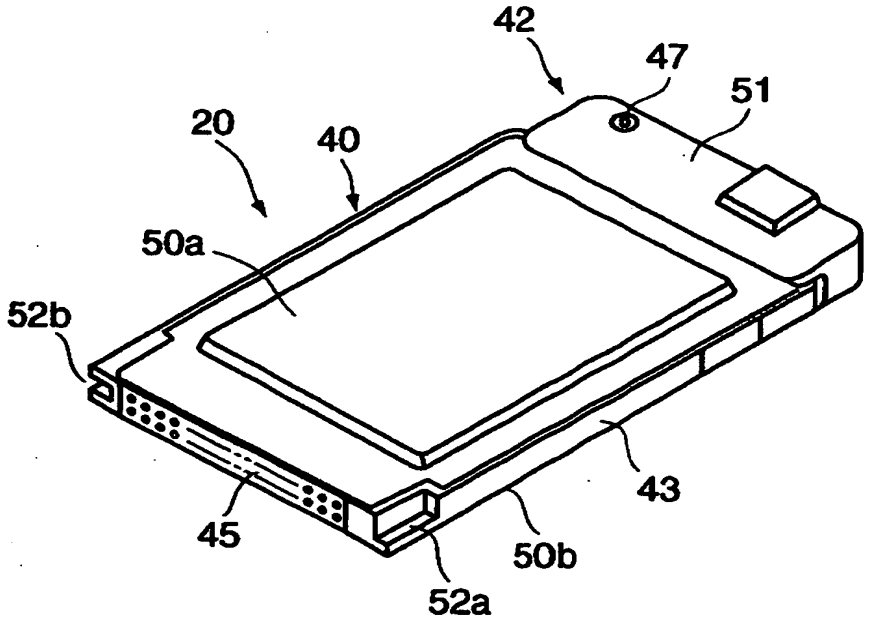
【図５】


10
14a
14e
24
37
14d
30
47
23
20
14c
22
48
42
51

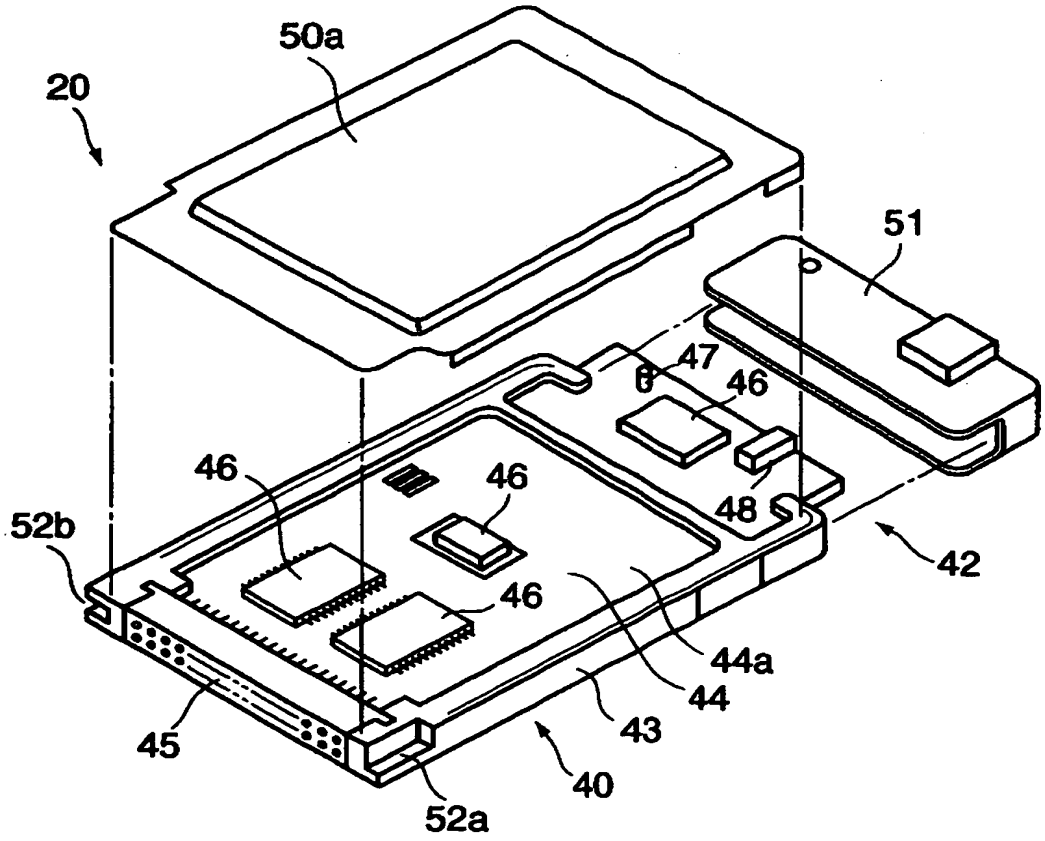
【図６】


10
34a
14e
36
34b
35
14
32
37
14b
14c

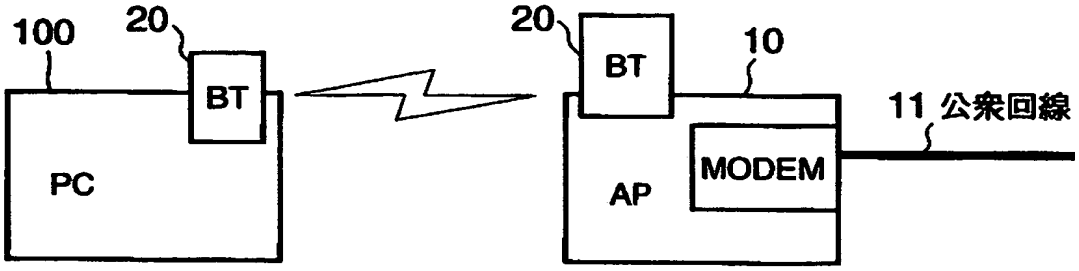
【図７】


42
47
51
20
40
50a
52b
43
45
50b
52a

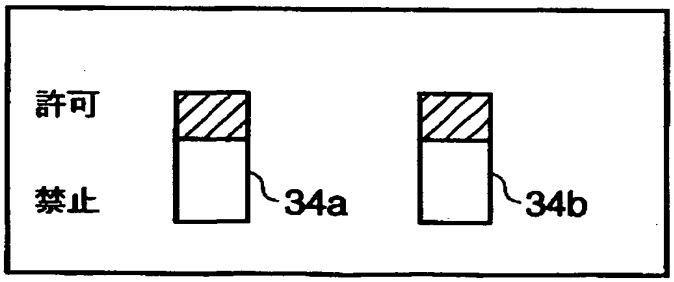
【図８】


50a
20
51
47
46
46
46
46
48
52b
42
44a
44
43
45
40
52a

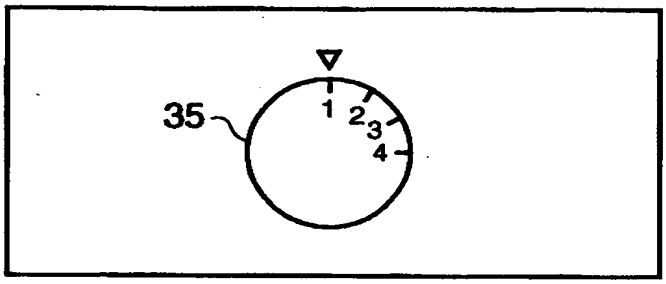
【図９】



【図１０】



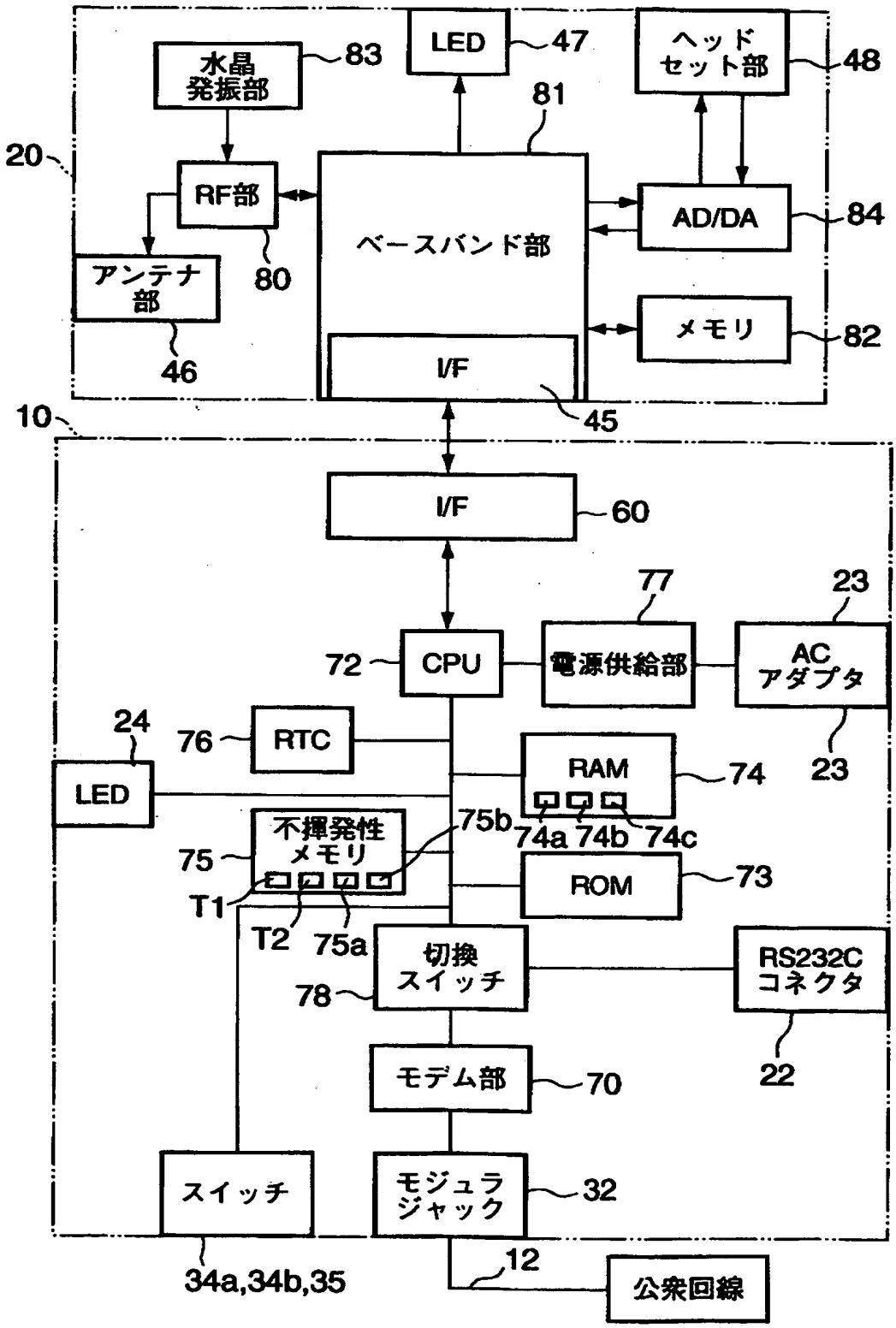
【図１１】



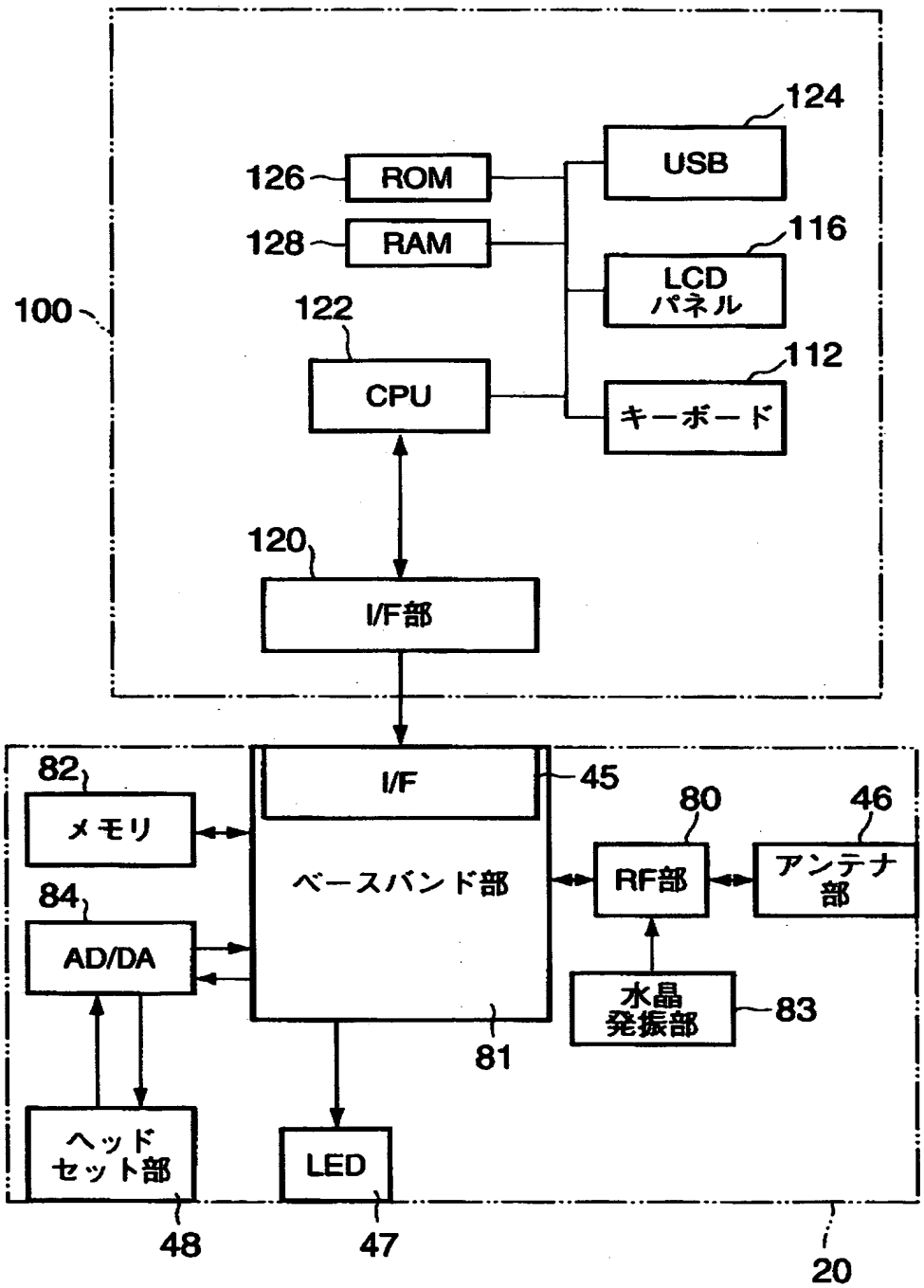
【図１２】

SW1	SW2	ロータリースイッチ
OFF	OFF	1
ON	OFF	2
OFF	ON	3
ON	ON	4

【図１３】


水晶
発振部
83
LED
47
ヘッド
セット部
48
81
20
RF部
ベースバンド部
AD/DA
84
アンテナ
部
80
メモリ
82
46
I/F
45
10
I/F
60
77
23
72
CPU
電源供給部
AC
アダプタ
24
76
RTC
LED
RAM
74
23
不揮発性
メモリ
75b
74a
74b
74c
75
ROM
73
T1
T2
75a
切換
スイッチ
RS232C
コネクタ
78
22
モデム部
70
スイッチ
モジュラ
ジャック
32
12
34a,34b,35
公衆回線

【図１４】


124
USB
126
ROM
128
RAM
116
LCD
パネル
100
122
CPU
112
キーボード
120
I/F部
82
メモリ
I/F
45
80
46
ベースバンド部
RF部
アンテナ
部
84
AD/DA
水晶
発振部
83
81
ヘッド
セット部
LED
48
47
20

【図１５】

T1 リンクテーブル

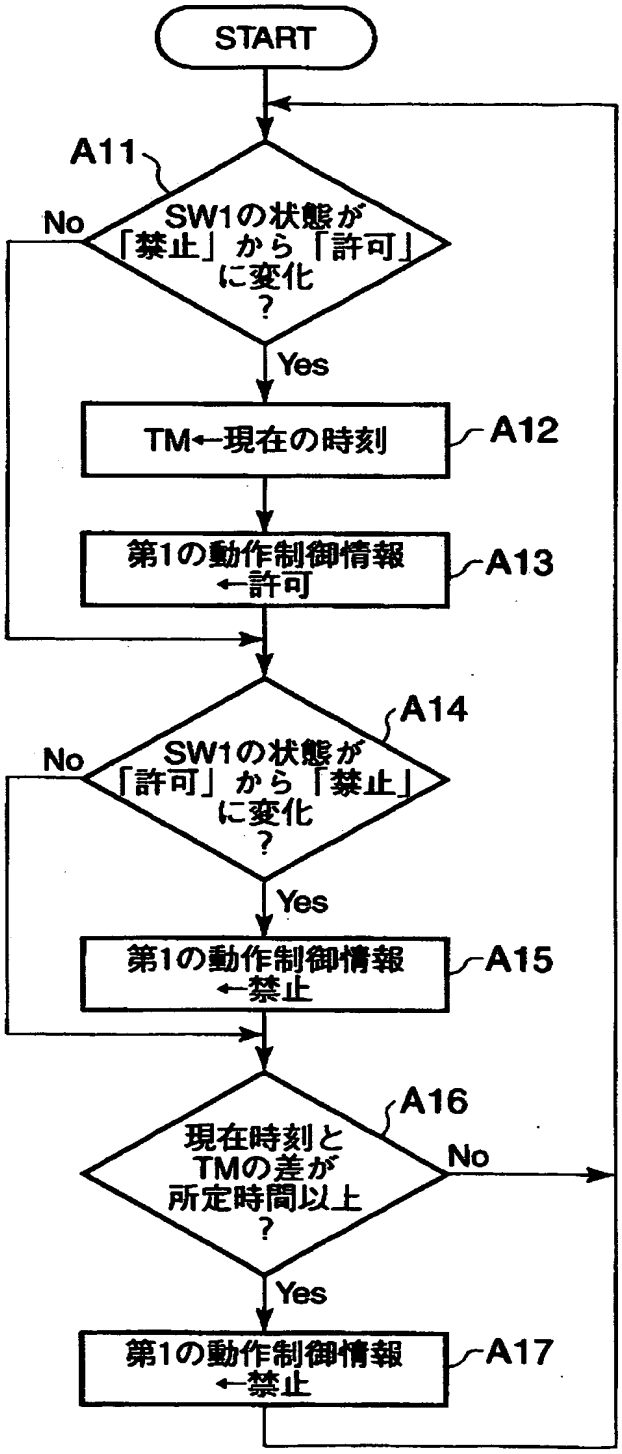
番号	ID (Hex)	ﾘﾝｸｷｰ	最終接続時刻	ﾃﾞｰﾀ有無ﾌﾗｸﾞ
1	A36B35	XXXXXX	2000/07/20/12:00:10	有
2	4B3346	xxxxxx	2000/05/20/11:00:07	有
	｜ ｜	｜ ｜		
N-1	87647A	oooooo	2000/08/12/16:30:37	有
N	—	—		無

【図１６】

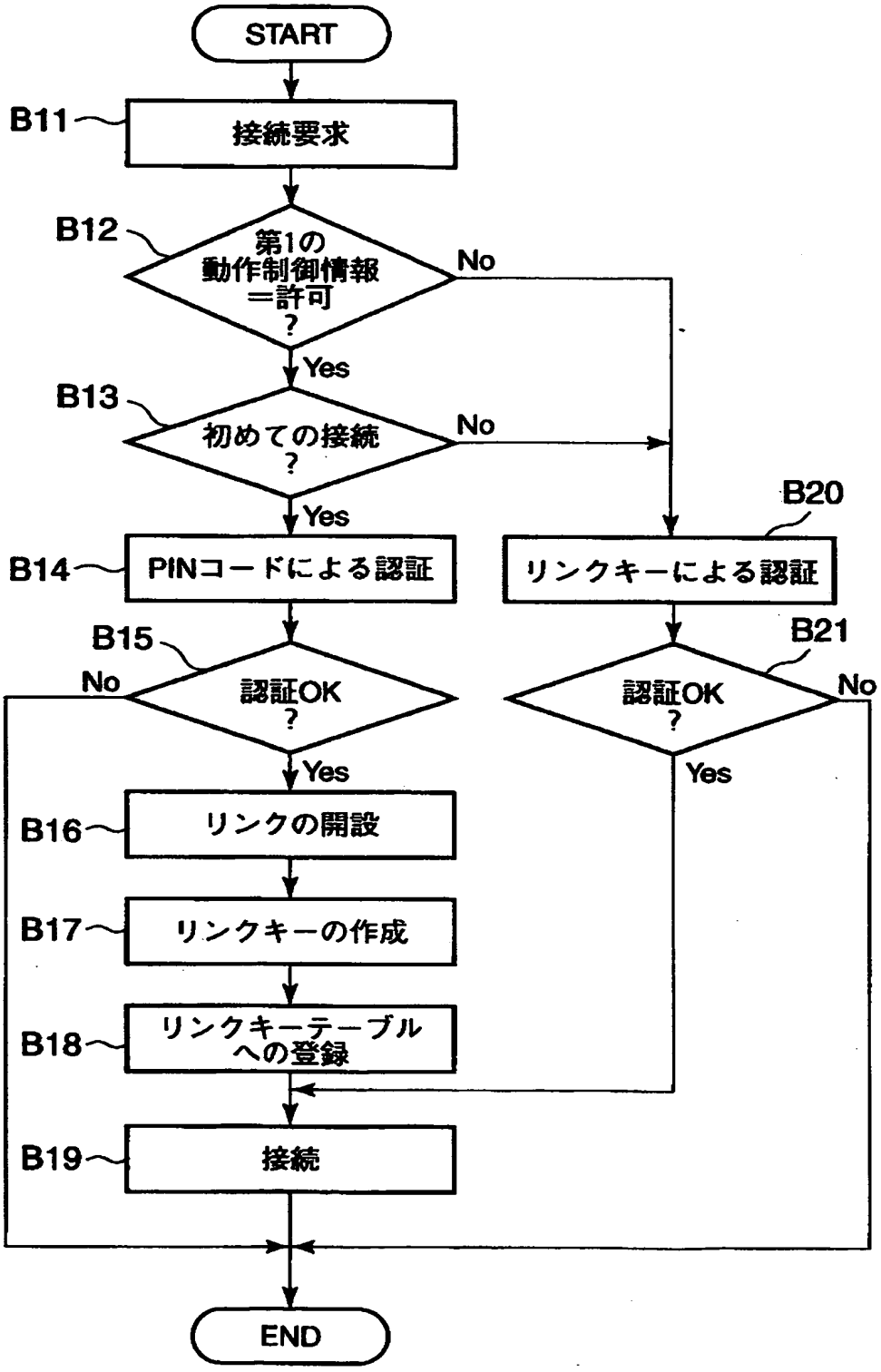
T2 認証エラーテーブル

番号	ID (Hex)	認証ｴﾗｰ回数	最終接続時刻	ﾃﾞｰﾀ有無ﾌﾗｸﾞ
1	A36B35	2	2000/07/20/12:00:10	有
2	4B3346	5	2000/05/20/11:00:07	有
	｜ ｜	｜ ｜		
M-1	87647A	1	2000/08/12/16:30:37	有
M	—	—		無

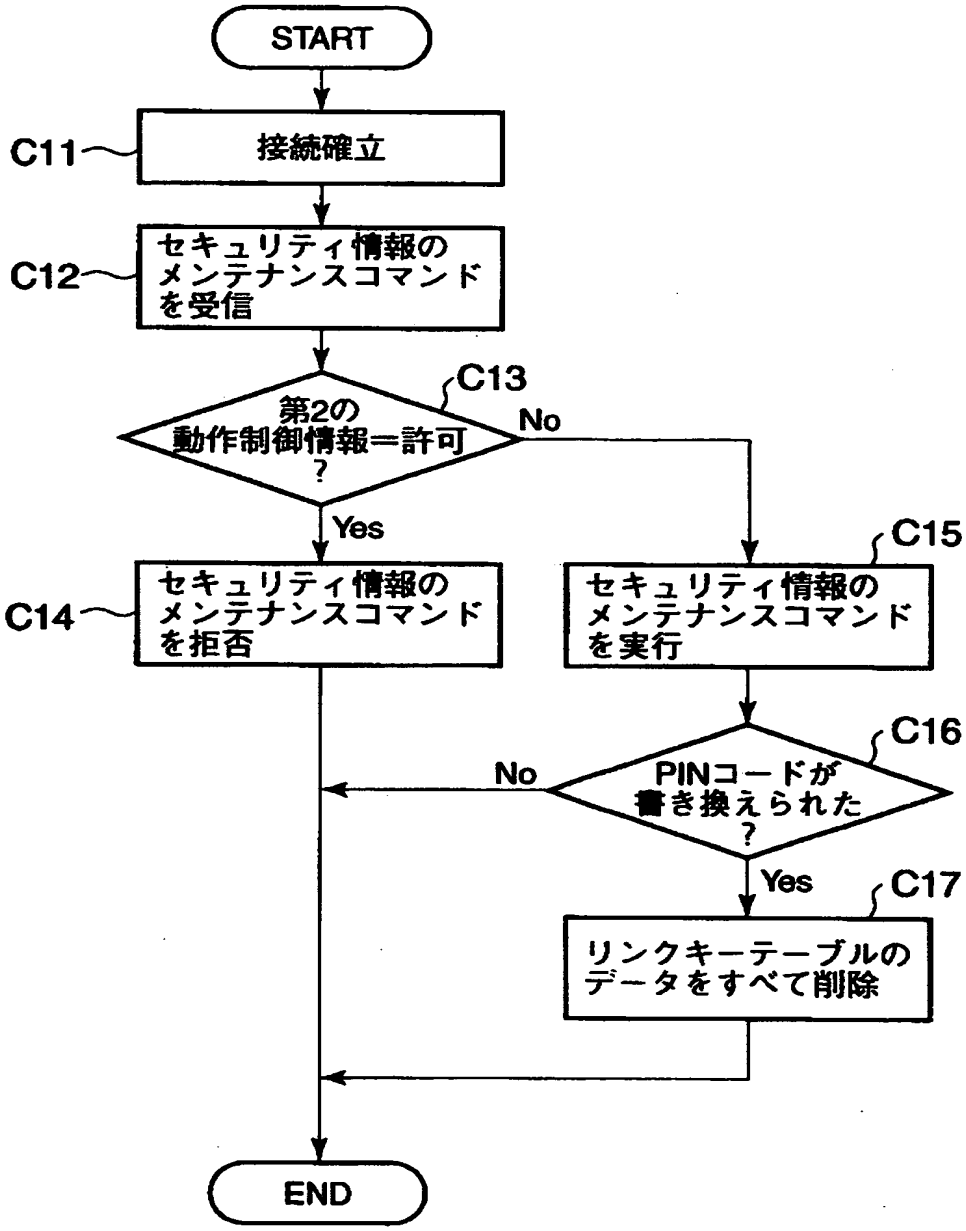
【図１７】


START
A11
SW1の状態が「禁止」から「許可」に変化？
No
Yes
TM←現在の時刻
A12
第1の動作制御情報←許可
A13
A14
SW1の状態が「許可」から「禁止」に変化？
No
Yes
第1の動作制御情報←禁止
A15
A16
現在時刻とTMの差が所定時間以上？
No
Yes
第1の動作制御情報←禁止
A17

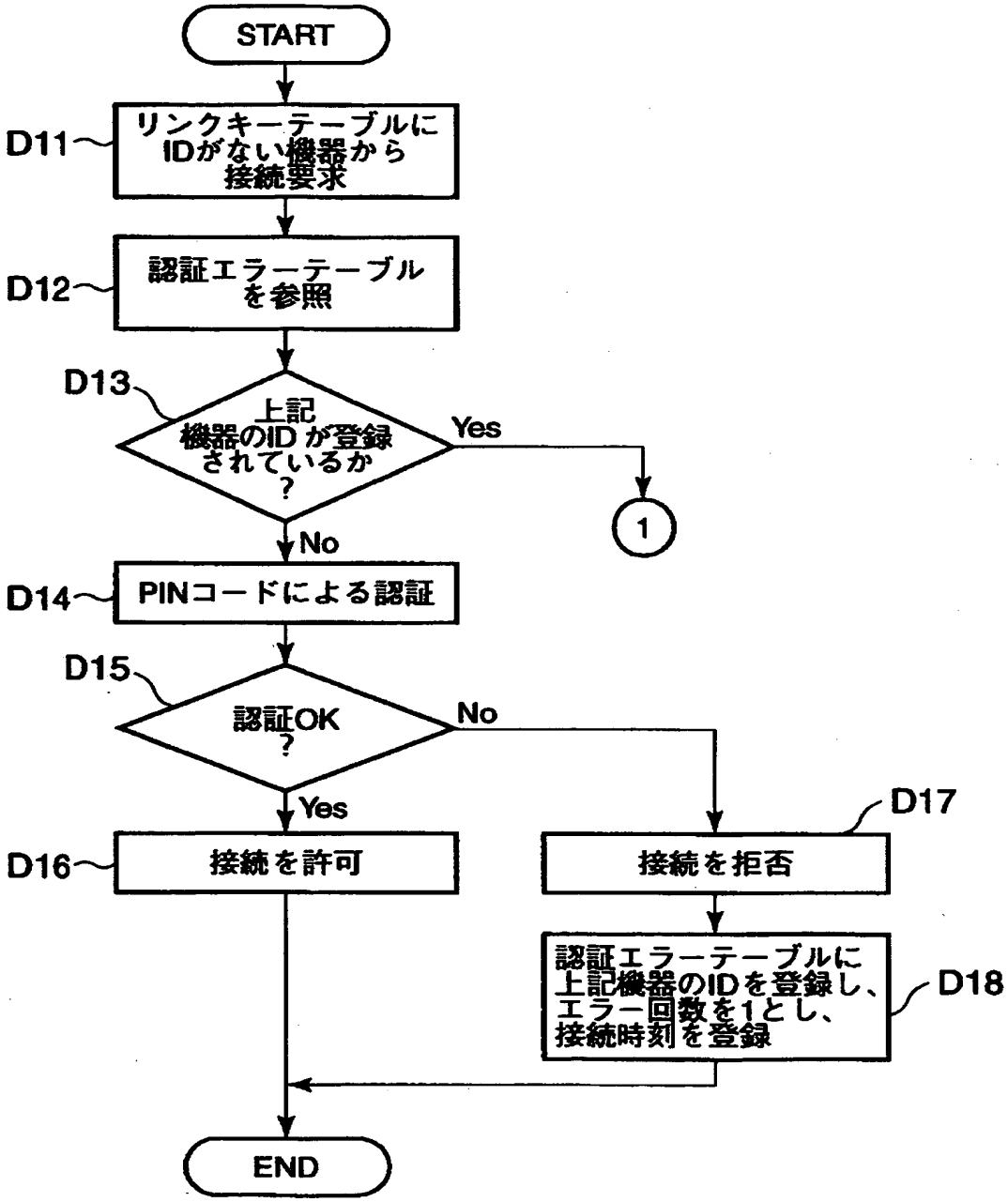
【図１８】


START
B11
接続要求
B12
第1の
動作制御情報
＝許可
?
No
Yes
B13
初めての接続
?
No
Yes
B20
B14
PINコードによる認証
リンクキーによる認証
B15
B21
No
認証OK
?
認証OK
?
No
Yes
Yes
B16
リンクの開設
B17
リンクキーの作成
B18
リンクキーテーブル
への登録
B19
接続
END

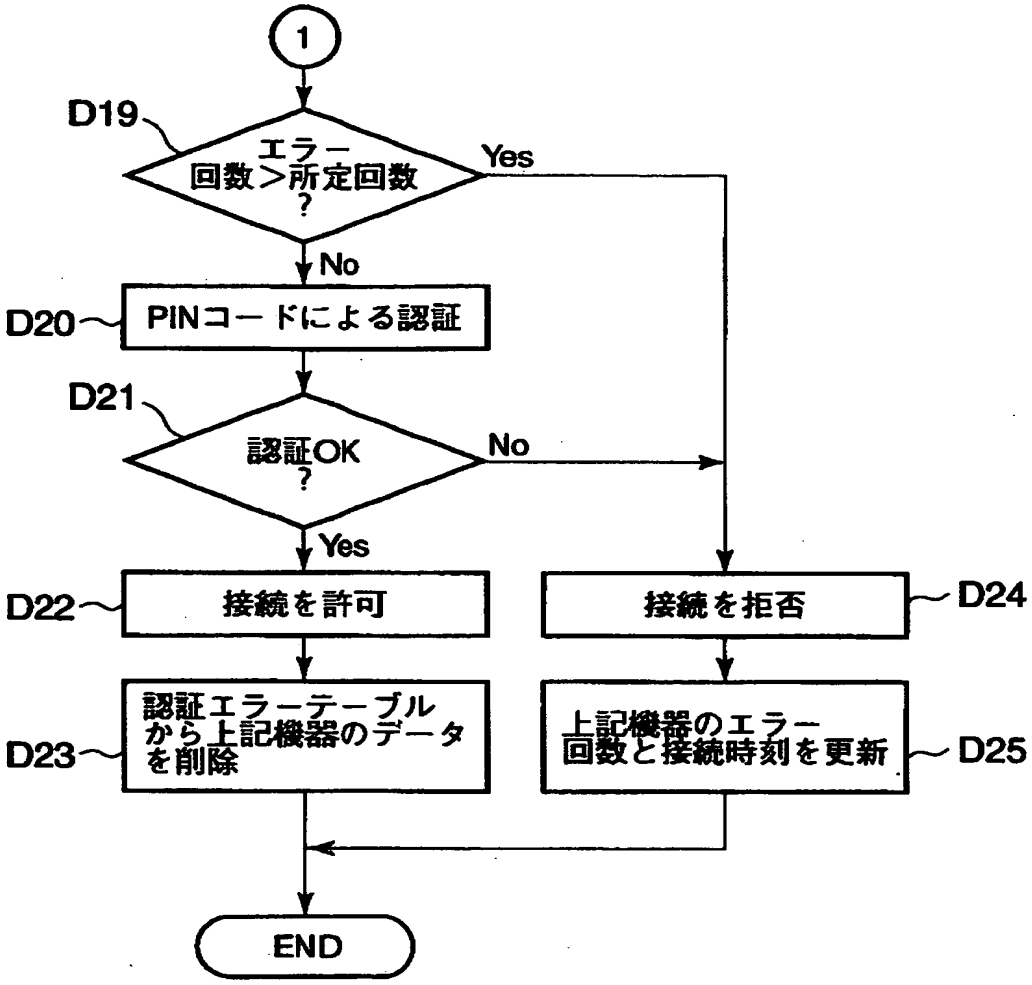
【図１９】


START
C11
接続確立
C12
セキュリティ情報のメンテナンスコマンドを受信
C13
第2の動作制御情報＝許可？
No
Yes
C14
セキュリティ情報のメンテナンスコマンドを拒否
C15
セキュリティ情報のメンテナンスコマンドを実行
C16
PINコードが書き換えられた？
No
Yes
C17
リンクキーテーブルのデータをすべて削除
END

【図２０】

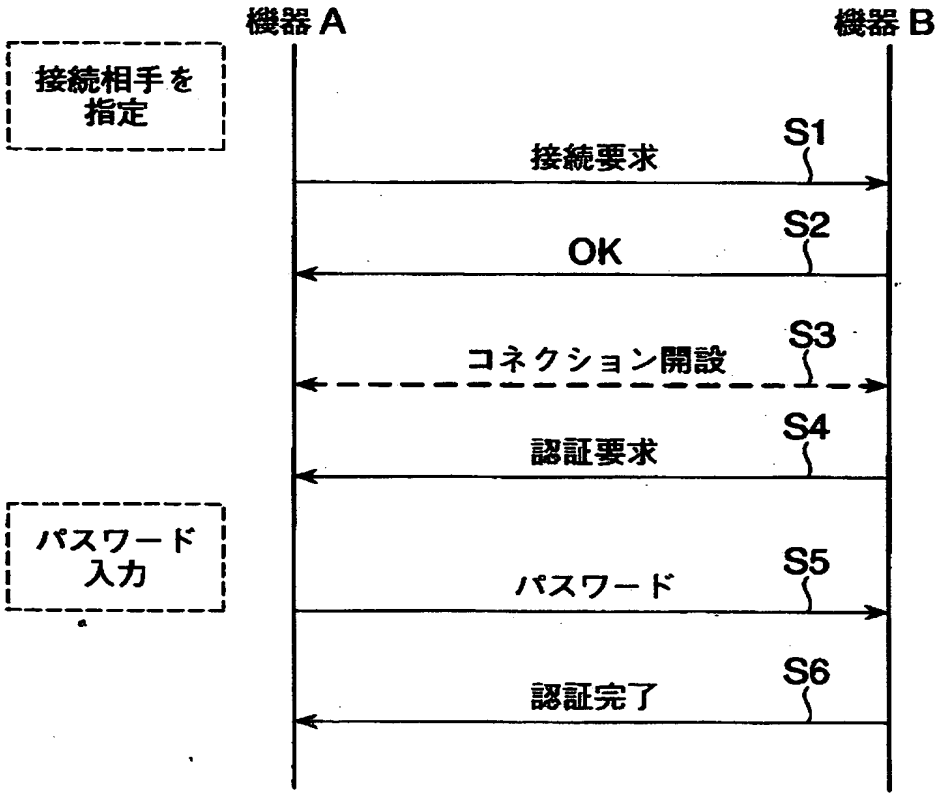

START
D11
リンクキーテーブルに
IDがない機器から
接続要求
D12
認証エラーテーブル
を参照
D13
上記
機器のIDが登録
されているか
?
Yes
1
No
D14
PINコードによる認証
D15
認証OK
?
No
Yes
D16
接続を許可
D17
接続を拒否
認証エラーテーブルに
上記機器のIDを登録し、
エラー回数を1とし、
接続時刻を登録
D18
END

【図２１】


1
D19
エラー回数＞所定回数？
Yes
No
D20
PINコードによる認証
D21
認証OK？
No
Yes
D22
接続を許可
接続を拒否
D24
D23
認証エラーテーブルから上記機器のデータを削除
上記機器のエラー回数と接続時刻を更新
D25
END

【図２２】

〔接続要求から認証完了までの流れ〕



【書類名】　　要約書

【要約】

【課題】他の機器からの不正アクセスを防止してセキュリティを確保する。

【解決手段】機器本体にスイッチを設け、このスイッチが許可状態に切り換えられた場合には、特定の識別コード（ＰＩＮコード）による認証を許可し（ステップＡ１１～Ａ１３）、スイッチが禁止状態に切り換えられた場合には上記特定の識別コードによる認証を禁止する（ステップＡ１４、Ａ１５）。これにより、普段はスイッチを禁止状態にしておくことで、不正アクセス者が特定の識別コードを用いてアクセスすることを防ぐことができる。また、スイッチが許可状態にあるときから所定時間経過した場合に、上記特定の識別コードによる認証を禁止する（ステップＡ１６、Ａ１７）。これにより、スイッチを許可状態にした後で禁止状態に戻し忘れたとしても、不正アクセスを防いで機器のセキュリティを確保できる。

【選択図】　　図１７

出 願 人 履 歴 情 報

識別番号　〔０００００３０７８〕

１．変更年月日　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝